Intermediate System Administration for the Solaris™ 9 Operating Environment SA-239

Student Guide



Sun Microsystems, Inc. UBRM05-104 500 Eldorado Blvd. Broomfield, CO 80021 U.S.A.

Revision A.2

Copyright 2003 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Sun, Sun Microsystems, the Sun logo, Java, Solaris, Ultra, SunOS, Sun StorEdge, ToolTalk, SunSolve, SunService, Sun Blade, Sun Enterprise, OpenBoot, Sun Fire, and JumpStart are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

PostScript is a trademark or registered trademark of Adobe Systems, Incorporated, which may be registered in certain jurisdictions.

Federal Acquisitions: Commercial Software - Government Users Subject to Standard License Terms and Conditions

Export Laws. Products, Services, and technical data delivered by Sun may be subject to U.S. export controls or the trade laws of other countries. You will comply with all such laws and obtain all licenses to export, re-export, or import as may be required after delivery to You. You will not export or re-export to entities on the most current U.S. export exclusions lists or to any country subject to U.S. embargo or terrorist controls as specified in the U.S. export laws. You will not use or provide Products, Services, or technical data for nuclear, missile, or chemical biological weaponry end uses.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

THIS MANUAL IS DESIGNED TO SUPPORT AN INSTRUCTOR-LED TRAINING (ILT) COURSE AND IS INTENDED TO BE USED FOR REFERENCE PURPOSES IN CONJUNCTION WITH THE ILT COURSE. THE MANUAL IS NOT A STANDALONE TRAINING TOOL. USE OF THE MANUAL FOR SELF-STUDY WITHOUT CLASS ATTENDANCE IS NOT RECOMMENDED.

Export Commodity Classification Number (ECCN) assigned: 12 December 2001

SA239_A2_0903_2_F





Copyright 2003 Sun Microsystems Inc. 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il v en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Sun, Sun Microsystems, the Sun logo, Java, Solaris, Ultra, SunOS, Sun StorEdge, ToolTalk, SunSolve, SunService, Sun Blade, Sun Enterprise, OpenBoot, Sun Fire, et JumpStart sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pavs.

Toutes les marques SPARC sont utilisées sous licence sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

UNIX est une marques déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

PostScript est une marque fabrique d'Adobe Systems, Incorporated, laquelle pourrait être déposée dans certaines juridictions.

Législation en matière dexportations. Les Pr duits, Services et données techniques livrés par Sun peuvent être soumis aux contrôles américains sur les exportations, ou à la législation commerciale dautres pays. Nous nous conformerons à lensemble de ces textes et nous obtiendrons toutes licences dexportation, de ré-exportation ou dimportation susceptibles dêtre requises après livraison à Vous. Vous nexporterez, ni ne ré-exporterez en aucun cas à des entités figurant sur les listes américaines dinterdiction dexportation les plus courantes, ni vers un quelconque pays soumis à embargo par les Etats-Unis, ou à des contrôles anti-terroristes, comme prévu par la législation américaine en matière dexportations. Vous nutiliserez, ni ne fournirez les Produits, Services ou données techniques pour aucune utilisation finale liée aux armes nucléaires, chimiques ou biologiques ou aux missiles.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

CE MANUEL DE RÉFÉRENCE DOIT ÊTRE UTILISÉ DANS LE CADRE D'UN COURS DE FORMATION DIRIGÉ PAR UN INSTRUCTEUR (ILT), IL NE S'AGIT PAS D'UN OUTIL DEFORMATION INDÉPENDANT. NOUS VOUS DÉCONSEILLONS DE L'UTILISER DANS LE CADRE D'UNE AUTO-FORMATION.





Table of Contents

About This Course	Preface-xix
Instructional Goals	Preface-xix
Course Map	Preface-xx
Topics Not Covered	Preface-xxi
Topics Not CoveredHow Prepared Are You?	Preface-xxii
Introductions	Preface-xxiii
How to Use Course Materials	Preface-yyiy
Conventions	Preface-xxv
Icons	Preface-xxv
Conventions	Preface-xxvi
Introducing the Solaris™ OE Directo	
Objectives	1_1
Introducing / (root) Subdirectories	
	n Directories 1-3
Introducing File Components	
	1-6
Identifying File Types	
	1-9
	1-10
	1-10
,	1-11
Using Hard Links	
	1-17
	1-17
	1-19
Performing the Exercises	
Exercise: Identifying File Types (Lo	
1	1-21

Exercise: Identifying File Types (Level 2)
Preparation1-22
Task Summary
Tasks 1-23
Exercise: Identifying File Types (Level 3)
Proparation1-25
Task Summary 1-25
Tasks and Solutions 1-26
Exercise Surranary1-29
Managing Local Disk Devices2-1
Objectives 2-1
Introducing the Basic Architecture of a Disk
Physical Disk Structure
Data Organization on Disk Platters 2-3
Disk Slices
Introducing Solaris Of: Oerice Naming Conventions2-11
Logical Device Names
Physical Device Names
Instance Names2-14
Listing a System's Devices 2-15
The /etc/path_to_inst File
The process Command 2-17
The format Command 2-17
Reconfiguring Devices 2-19
Performing a Reconfiguration Boot
Using the devfsadm Command
Performing the Exercises
Exercise: Configuring and Naming Devices (Level 1)2-23
Preparation
Tasks
Berose Configuring and Naming Devices (Le el 2)2-24
Preparation2.24
Task Summary 2.24
Tasks
Exercise: Configuring and Nanting Devices (Level 3)2-27
Preparation2-27
Task Summary2-27
Tasks and Solutions 2.28
Exercise Summary
Partitioning the Hard Disk
Infroducing the Fundamentals of Disk Partitioning2-32
Recognizing Disk Space and Undesirable Conditions 2-33
Recognizing Wasted Disk Space2-34
Recognizing Overlapping Disk Slices
Introducing Disk Partition Tables

	Using the format Command	2-37
	Partitioning a Disk	2-39
	Saving a Partition Table to the /etc/format .dat File	2-45
	Using the Customized Partition Table	2-16
	Managing Disk Labels	
	Viewing the Disk VTOC	
	Relabeling a Disk	
	Performing the Exercises	
	Exercise: Working With Disks and Partitions (Level 1)	
	Preparation	
	Tasks	
	Exercise: Working With Disks and Partitions (Level 2)	2-54
	Preparation	
	Task Summary	
	Taslas	2-55
	Exercise: Working With Disks and Partitions (Level 3)	2-58
	t'reparation	
	Task Summary	2-58
	Tasks	
	Introducing the Solaris™ Management Console,	2-66
	Starting the Solaris Management Console	2-66
	Using the Solaris Management Congale Tools	2-67
	Restarting the Solaris Management Console	
	Identifying the Functional Areas of the Solaris	
	Management Console	2-64
1988 18	Partitioning a Disk by Using the Solaris Management	
William &	Console Disks Manager Tool	2-73
	Partitioning the Disk Using the Disks Tool	2-73
	Performing the Exercises	2-82
	Exercise: Working With the Solaris Management Consule	
	(Level 1)	2- 83
	Preparation	2-83
	Tasks	2-63
	Exercise: Working With the Solaris Management Console	
	(Level 2)	2-84
	Preparation	2-84
	lask Summary	
	Tasks	2-H4
	Exercise Survey	_2-86
Mai	naging the Solaris OE File System	3.1
	• Directives	
	Introducing Solaris OB File Systems	
	Disk-based File Systems	
	Distributed File Systems	
	Prando Filo Systems	

Creating a New uis File System3-4
Viewing the Solaris OE us File System
Using the newEs Command
Checking the File System by Using the fack Command 3-16
Data Inconsistencies Checked by the fack Command 3.16
Superblock Consistency3-16
Cylinder Group Block Consistency
Inode Consistency
Data Block Consistency
The last +found Directory
Nominteractive Mode 3-17
Interactive Mode
Resolving File System inconsistencies
Reconnecting an Allocated Unreferenced File
Adjusting a Link Counter 3-20
Salvaging the Free List
Using Backup Superblocks 3-21
Monitoring File System Use
Using the df Command 3-23
Using the du Connegad
Using the que - Command. 3-26
Using the Solaris Management Console Usage Tool 3-27
Performing the Exercises3-29
Exercise: Creating & Maintaining ufs File Systems
(Level 1)
Preparation3-30
Tasks
Exercise: Creating and Mairdaining of File Systems
(Level 2)3-32
Preparation3-32
Task Summary
Tasks
Exercise: Creating and Maintaining ufs File Systems
(Level 3)
reparation
Task Summary
Tasks and Solutions
Exercise Summary 3-4
Performing Mounts and Unmounts
Objectives 4-1 Working With Mounting Fundamentals 4-2
Determining Which File Systems Are Currently
Mounting a File System Autumatically
PROUNDING & FILE DYSTEM ACTOMATICALLY

	Introducing the Virtual File System Table:	
	/etc/Vfstab	4-4
	Introducing the /etc/amatab File	4-6
	Performing Mounts	4-8
	Mounting a Local File System Manually	4-8
	Using the mount Command Options	
	Mounting All File Systems Manually	
	Mounting a New File System	
	Mounting Different Types of File Systems	
	Performing Unmounts	
	Unmounting a File System	
	Unmounting All File Systems	
	Un mounting a Busy File System	4-17
	Repairing Important Files if Boot Fails	4-19
	Accessing Mounted Diskettes and CD-ROMs	4-21
	Using Volume Management	4 - 22
	Restricting Access to Mounted Disketter and CD-ROMs	
	Stopping Volume Management	
	Troubleshooting Volume Management Problems	
	Accessing a Diskette or CD-ROM Without Volume	4-44
	Management	4_25
	Using the mount Command	4-20
	Performing the Exercises	4 26
	Exercise: Mounting File Systems (Level 1)	1.27
	Preparation	
a Table w	Tasks	
	Exercise: Mounting File Systems (Level 2)	4_29
	Preparation	4.20
	Pask Summan	1.70
	Tasks	
11 日音像	Exercise: Mounting File Systems (Level 3)	
	Preparation	4.42
	Task Summary	
THE RESERVE	Tasks and Solutions	
	Exercise Summary	
Inst	alling the Solaris™ 9 Operating Environment	5-1
	Object yes	5- l
	Identifying the Fundamentals of the CD-ROM Installation	···5·2
	Solaris 9 OE Installation and Lipgrade Options	5-2
	Solaris Web Start 3.0 Installation Software	
	Custom JumpStart M Installation	
	Solaris Web Start Flash Installation Software	
	Standard Upgrade to the Solaris QE	5-4
	Solaris Live Upgrade Software	5-4
	Hardware Requirements for Installation of the	
	Solaria 9 OE	5-4

Software Components of the Solaris OE	5-5
Solaris OE Software Groups	5-6
Installing the Solaris 9 OE From a CD-ROM	5.9
Pre-Installation Information	
Demonstration: Performing an Interactive	
Installation	11
Performing Solaris 9 OE Package Administration	
Performing Solaris & OE Package Administration)- II
Objectives)-L
Introducing the Fundamentals of Package Administration	1-2
Software Packages	
The /var/audo/install/contents File(
Administering Packages From the Command Line)- - - - +
Displaying Information About lustailed Software	
Packages	, 7
Ad ing a Software Package	
Checking a Package Installation	ກຕ
Removing a Software Package6-	10
Adding Packages by Using a Spool Directory 6-	
Reviewing Package Administration 6-	13
Performing the Exercises 35	14
Fxercise: Manipulating Software Packages (Level 1)6-Preparation 6-	15
Preparation 6-	15
Tasks 6-	15
Exercise: Manipulating Software Packages (Level 2)	
PreParation 6-	16
Task Summary0-	10
Tasks 6-	16
Exercise: Manipulating Software Packages (Level 3)6-	
Preparation6-	
Task Summary 6-	
Tasks and Solutions6-	
Exercia Si minary 6-	21
Managing Software Patches on the Solaris 9 OE7	'-1
Objectives	
Preparing for Patch Administration	
Introducing Solaris OE Patches	
Checking Patch Levels	
Obtaining Patches	
Preparing Palches for Instellation	7-7
Installing and Removing Patches	7-9
Installing a Patch	
Removing a Patch	
Installing Patch Clusters	
Performing the Exercises	

Exercise: Maintaining Patches (Level 1)	7-1 7
Preparation	7-17
Tagle	7-17
Exercise: Maintaining Patches (Level 2)	7-18
Preparation	
Task Summary	7- 18
Taska	7-19
Exercise: Maintaining Fatches (Level 3)	7-20
Preparation	7-20
Task Summary	 7-2 0
Tasks and Solutions	
Exercise Summary	
Executing Boot PROM Commands	
Objectives	
Introducing Boot PROM Fundamentals	8 7
Goal of the OpenBoot Architecture Standard	
Boot PROM	
NRAM	#.=
COSP	
Disabling the Abod Samura	
Disabling the Abort SequenceDisPlaying I'QST to the Serial Port	о-о
Using Basic Boot PROM Commands	رجی 1 1 م
Identifying the System Boot PROM Version	11-دمد 1.7
Booting the System	
Accessing More Detailed Information	
Listing NVRAM Parameters	
Changing NVRAM Parameters	G 14
Restoring Default NORAM Parameters	
Displaying Devices Connected to the Bus	
Identifying the System's Boot Device	
The st.ew-devs Command	P 23
The devalues Command	⊕ 7.4
Creating and Removing Custom Device Aliases	0 15
Citating and Removing Custom Device Aliases	0-23
The river lies Command	e 26
Viewing and Changing NVRAM Parameters From the	0-40
	ט מי
5hcll	
Using the eeprow.Command	0.20
Interrupting an Unresponsive System	0.20
Aborting an Unresponsive System	
Performing the Exercises Exercise: Using the OpenBoot PROM Commands	8-29
	ບ່າ
(Level 1)	0
Preparcition	
Taska	\$-30

	Exercise: Using the OpenBoot PROM Commands	
	(Level 2)	S-32
	Preparation	8-32
	Task Summary	
	Tasks	
	Exercise: Using the OpenBoot PROM Commands	
	(Level 3)	8-36
	Preparation	
	l'ask Summary	
	Tasks and Solutions	8-37
	Exercise Simmary	
Daz	forming Boot and Shutdown Procedures	
1 61	Objectives	
	Identifying Run Level Fundamentals	9.7
	Solatis Oli Run Levels	9_7
	Determining a System's Current Run Level	0.3
	Changing Run Levels	9.3
	Changing Run Levels	u 1
	Boot PROM Phase	9-5
	Boot Programs Phase.	9.5
	The kernel huitialization Phase	9-6
	The /esc/systemFile and kernel Configuration	
	The init Phase	
	Controlling Boot Processes	
	The /spin Directory	
	The /etc/rc# d Directories	9-20
	Start Run Control Scripts	
Character 1	Stop Run Control Scripts	
	The /etc/init.d Directory	
	Creating New Run Control Scripts	
	Performing System Shutdown Procedures	
	The /usr/sbin/init Command	9-26
	The /:sr/sbin/shutdown Command	
	The / her/spin/halt Command	
	The /usr/sbin/poweroff Command	
	The /usz/sbin/remoot Command	
	Performing the Exercises	
	Exercise: Controlling the Boot Process (Level 1)	9,34)
	Preparation	
	Tasks	
	Exercise: Controlling the Boot Process (Level 2)	
	treparation	
	Task Summary	
	Tasks	

	Exercise: Controlling the Boot Process (Level 3)	9-34
	Preparation	9-34
	Task Summary	9-34
	Tasks and Solutions	9-35
	Fixercise Summary	9-38
Po	erforming User Administration	10-1
	Objectives	10-1
	Introducing User Administration	10-2
	Main Components of User Account	1()-2
	System Files That Store User Account Information	
	Managing User Accounts	10-11
	Introducing Command-Line Tools	10-11
	Creating a User Account	10-13
	Modifying a User Account 3x	10-16
	Deleting a User Account	
	Creating a Group Entry	
	Medifying a Group Entry	
	Deleting a Group Entry	
	Using the Solaris Management Console Users Tool	
	Troubleshooting Login Issues	1032
	Performing the Exercises	10- 6
	Exercise: Adding User Accounts and Group Entrics	
	(Level 1)Preparation	10-37
	Preparation	10-37
	Tasks	10-38
	Exercise: Adding User Accounts and Group Entries	
	(Level 2)	10-40
	Preparation	10-4()
	Task Summary	10-40
	Tasks	10-41
	Exercise: Adding User Accounts and Group Entries	
	(Level 3)	10-45
	Preparation	10-45
	Task Summary	
	Tasks and Selations	10-46
	Exercise Summary	
	Managing Initialization Files	10-53
	Introducing System-Wide Initialization Files	10-53
	Introducing User Initialization Files	
	Customizing the User's Work nvironment	
	Ferforming the Exercises	
	Exercise: Modifying Initialization Files (Level 1)	
	Preparation	
	Tooks	10 =0

Exercise: Modifying Initialization Files (Level 2)	10-60
Preparation	
Task Summary	10-60
Tasks	10-61
Exercise: Modifying Initialization Files (Level 3)	10-63
Preparation	10-63
Task Summary	10-6.3
Tasks and Solutions	
Exercise Summary	10-67
Performing System Security	11-1
Objectives	
Monitoring System Access	
Displaying Users on the Local Systems	
Displaying Users on Remote Systems	
Displaying User Information	11-4
Displaying a Record of Login Activity	11 -5
Recording Failed Login Attempts	11-6
Switching Users on a System	220000000000000000000000000000000000000
Introducing the su Command	11-7
Introducing the su Command Switching to Another Regular User	11-9
Beconging the root User	
Monitoring s: Attempts	
Controlling System Acress	11_13
The /etc/default/login File	
File Transfer Protocol (FTP) Access	
The /etc/hosts.equivand \$HOME/, rhosts Fil	
The /etc/hosts.equivFile Rules	
The \$FORE/ rhosts File Rules	
Performing the Exercises	
Exercise: User Acress (Level 1)	11-21
Preparation	
Tasks	
Exercise: User Access (Level 2)	
Preparation	
Task Summary	11-23
Tasks	
Exercise: User Access (Level 3)	11-27
Preparation	
Task Summary	11-27
Tasks and Solutions	
Exercise Summary	
Restricting Access to Data in Files	
Determining a User's Group Membership	
ldentifying a User Account	
Changing life and Directors Opmership	

Changing File and Directory Group Membership.	
Using File Permissions	
Performing the Exercises	
Exercise: Restricting Access to Data on Systems (Level :	1) 11-44
Preparation	11-44
Tasks	11-44
Exercise: Restricting Access to Data on Systems (Level 2	2) 1116
Preparation	
Task Summary	
Tasks	
Exercise: Restricting Access to Data on Systems (Level 3	
Preparation	
Task Summary	
Tasks and Solutions	
Exercise Summary	
Canfiguring Printer Services	
Configuring Printer Services	12-1
•bjectives	12-1
Introducing Network Printing Fundamentals	
Print Management Tools	
Client-Server Model	
Types of Printer Configurations	
Basic Functions of the Solaris OE LP Point Service	12-5
LP Print Service Directory Structure	12-5
Solaris OE Printing Process	
Configuring Printer Services	
Identifying Print Server Requirements	
Using the Solaris @EPrint Manager	12-20
Configuring a New Network Printer	12-23
Administering Printer Services	12-31
Configuring Printer Classes	
Sciting the System's Default Printer	
Changing the System's Default Printer Class	
Removing a Client's Printer Configuration	12-35
Removing a Server's Printer Configuration	12-36
Starting and Stopping the LP Print Service	
Starting the LP Print Service	
Stopping the LP Print Service	12-37
Using Print Commands	13-1
Objectives	
Specifying a Destination Printer	
Using the 1 Command	
Using the IprCommand.	13-2
Using the LP Print Service	13.3
Accepting Print Jobs	
Rejecting Print Jobs	

	ling Printers		
Disa	bling Printers		13-5
Mov	ing Print Jobs		13-6
	g the Exercises		
	Jsing the LP Print S		
	aration		
	S		
	Using the LP Print S		
	त्तकोता		
	Summary		
	\$		
	Using the LP PrintS		
	aration		
	Summary		
	s and Scilutions		
	นานเสร		
			400
	stem Processes		
Objectives	ystem Processes	***************************************	14-1
Viewing S	ystem Processes		.,14-2
Usin	the CDI Process A	lanager	14-2
Usin	g the present Comun	ard	144
Usin	g the Solaris Managr	ement Console Proc	ess Tool 14-7
Clearing F	rozen Processes		14-9
Usin	g the kill and pkil	1 Commands	14-9
	orming a Remote Log		
Schedulin	g an Automatic One	-Time Execution of	a Command
14-12	The same of the sa		
Usin	g the at Command	J	14-12
Cont	rolling Access to the	at Command	14-14
Schedul'un	g an Automatic Reci	uring Execution of	a Command
14-15			
	ducing the crontab		
Usin	gthe crontabComi	miand	14.17
Cont	rolling Access to the	erentab Command	d 14-19
	g the Solaris TM Mana		
14-3			
Performin	g the Exercises		
Exercise: 1	Jsing Process Contr	ol (Level 1)	14-23
Prep	aration		14-2.3
Task	S	0111111100311110011003111110033111000311	14-23
Exercise: 1	Using Process Contro	ol (Level 2)	
	aration		
	Suconary		
т ,	#		112-

Exercise: Using Process Control (Level 3)	14-27
Preparation	14-27
Task Summary	
Tasks and Solutions	14-28
Exercise Sturmary	14-31
Performing File System Backups	
Objectives	
Introducing the Fundamentals of Backups	
Importance of Routine File System acku s	15-2
Tape Media Types	15-3
Tape Drive Naming	
Tape Drive Control	
Strategies for Scheduled Backups	15-6
The /etc/aumpdates File	15-9
Backing Up an Unmounted File System	15-10
The ufscump Command	15-16
Options for the ufadiant Command	15-11
Tape Back Ups	15-12
Remote Backups to a Tape	15-13
Performing the Exercises	15-14
Exercise: Backing apa File System (Level 1)	15-15
Preparation	15-15
Tasks	15-15
Exercise: Backing Up a File System (Level 2)	
Preparation	
Task Summary	
'Fasks	
Exercise: Backing Up a File System (Level 3)	
Preparation	15-18
Task Summary	15-18
Tasks and Solutions	
Exercise Summary	15-21
Performing File System Restores	16-1
Objectives	
Restoring a ufs File System	
Restoring a Regular File System	
Restoring the /use File System	
Performing a Special Case Recovery of the / (root)	
File System	10-0
Involving an Interactive Restore	
Performing an Incremental Restore	
Exercise: Recovering Backup Files and File Systems	mmer 11)-14
(Level 1)	16.19
Preparation	14.15
T 1 Z Pice alluint	

Evertise: Recovering Backop Files and File Systems	
(Level 2)	
Preparation	16-16
Task Summary	16-16
Taske	16-17
Exercise: Recovering Backup Files and File Systems	
(Level 3)	16-19
Preparation	16-19
Task Sunmary	
Tasks and Solutions	16-20
Exercise Summary	16-25
Introducing Disaster Recovery Fundamentals	16-26
Dieaster Scenarios That Can Result in a Loss of Data	16-26
Disaster Recovery Plan	16-26
Importance of Oit-Site Backups	16.30
Components Required to Operate a Hotsite.	16-31
Importance of Disaster Recovery Drills	l6-3l
Backing Up a Mounted File System With a UFS Snapshot	. 17-1
Objectives	. 17-1
Creating a UFS Snapshot .	. 17-2
Using the fss rapCommand	. 17-2
Linuting the Size of the Backing-Store File	
Displaying Information for a urs File System	
Snapshot	. 17-5
Backing Up the UFSSnapshot File	17.6
Performing a Backup of a UFS Snapshot	17-6
Performing an Incommental Backup of a UFS	
Strapshot	17-7
Restoring Data From a UFS Snapshot Backup	
Deleting a UFS Snapshot	17 -10
Performing the Exercises	17-TL
Bracke Working With UPS Snapshots (Level 1)	
Taks	
Exercise: Working With UPS Strapshots (Level 2)	
Task Survnary	17-13
tasks	17-13
Exercise: Working With UPS Seepshots (Level 3)	
Task Summary	
Tasks and Solutions	
Exercise Summary	17-15
IndexIndex	lex-1

Performing Boot and Shutdown Procedures

Objectives

Upon completion of this module, you should be able to:

- Identify run level fundamentals
- Identify the phases of the boot process
- Control boot processes
- Perform system shutdown procedures

The following course map shows how this module fits into the current instructional goal.

Performing System Boot Procedures

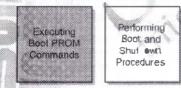


Figure 9-1 Course Map

Identifying Run Level Fundamentals

A run level is a system state, represented by a digit or letter, that defines what service and resources a mrently available to users. The system is always running in a single run level.

Solaris OE Run Levels

Table 9-1 shows the eight run levels found in the Solaris OE.

Table 9-1 olaris OE Run Levels

Run Level	Function
0	System is running the PROM monitor.
s or S	Solaris Olating excer mode with critical file systems mounted and accessible.
1	The system is running in a single-user administrative state with access to all available file systems.
2	The system is supporting multiuser operations. Multiple users can access the system All system daemons are running except for the Network File System (NFS) server and some other network resource server related daemons.
3	The system is supporting multiuser operations and has NFS resource sharing and other network resource servers available Specified as the default run level in the /etc/inittabfile.
4	This level is currently not implemented.
5	A transitional run level in which the Solaris OE is shut down and the system is powered off.
6	A transitional run level in which the Solaris OE is shut down and the system reboots to the default run level.

Determining a System's Current Run Level

To determine the current run level of a system, use the who incommand.

Figure 9-2 shows output from the command.

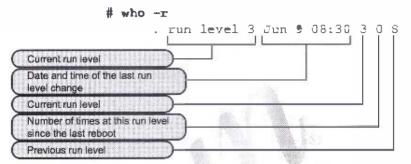


Figure 9-2 The System's Current Run Level

Changing Run Levels

Run levels are sometimes referred to as init states because the init process transitions between run levels. You can use the init command to manually initiate run-level transitions. You can also change run levels with the shurdown, halt, referent, and poweroff commands.

Identifying the Phases of the Boot Process

In general, when a system is powered on, the PROM monitor runs a POST procedure that checks the hardware and memory on the system. If no errors are found, and the auto-boot? parameter is set to true, the system bygins the automatic boot process.

The entire bool process is described by four distinct phases:

- The boot PROM phase
- The boot programs phase
- The kernel initialization phase
- The init phase

Figure 9-3 shows the phases of the boot process.

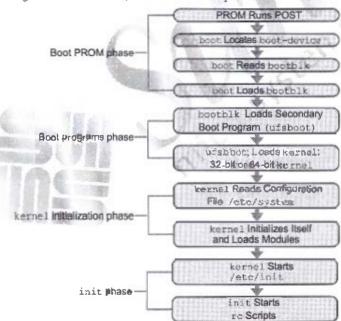


Figure 9-3 Phases of the Boot Process

Boot PROM Phase

The boot PROM performs the following steps during the first part of the boot sequence:

- The PROM runs the POST.
 - The boot PROM firmware runs the POST to verify the system's hardware and memory. It then begins its boot sequence upon successful completion of the self-test diagnostics.
- The PROM displays the system identification banner.
 - The model type, processor type and speed, keyboard status, PROM revision number, amount of installed random access memory (RAM), NVRAM serial number, Ethernet address, and host ID are displayed.
- The boot PROM determines the boot device by reading the PROM parameter boot-device.
- The boot PROM reads the disk label located at Sector 0 on the default boot device.
- The boot PROM finds the boot program from the default boot device programmed into the PROM.
 - The boot PROM program reads a system's primary boot program called bootblk (located at Sectors 1 through 15) that contains a UNIX file system (u.f.s) file system reader. (The bootblk program is placed on the chilk by the install boot program during system installation.)
 - The coor command leads the beetblk program from is location on the boot device into memory.

Boot Programs Phase

The following describes the boot programs phase:

- The hootably program loads the secondary best program, usabbet, from the boot device into memory.
 - The path to use oot is recorded in the bootblk program, which is installed by the Solaris OE unity installabor.
- The ofshoot program locates and loads the appropriate two-part kernel.

The core of the kernel is two pieces of static code called genunial and units where genunial is the platform-independent generic kernel file and units is the platform-specific kernel file.

When ufshoot loads these two files into memory, they are combined to form the running kernel.

On a system numing in 32-bit mode, the two-part kernel is located in the directory /placform/hunane -m'/kernel.

On a system running in 64-bit mode, the two-part kernel is located in the directory /platform/'uname -m'/kernel/sparcy9.



Note - To determine the platform name (for example, the system hardware class), type the uname -m command. For example, when you type this command on an Ultra 10 workstation, the console displays sun4u.

The kernel Initialization Phase

The following describes the kernel initialization phase:

- The kernel mads its configuration file, called /ecc/system.
- The kernel initializes itself and begins loading modules.
 The kernel uses the ufsboot command to load the files. When it has loaded enough modules to mount the root file system, it unmaps the visboot pro ran and con nues.
- The result starts the /etc/init process.



Note = The /eto/ir.it and /obin/init processes are linked together.

The SunOS^N serve is a small start core, cursisting of genuinx and unit and many dynamically loadable kernel modules.

Modules can consist of device drivers, binary files to support file systems, and streams, as well as other module types used for specific tasks within the system.

The modules that make up the kernel typically reside in the directorles/kernel and /war/kernel. Platform-dependent modules reside in the /wlatform/mname =m*/kernel and /platform/mname =i*/kernel directories.

Each subdirectory located under these directories (see Figure 9-4) is a collection of similar modules.

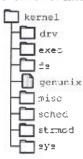


Figure 9-4 Medule Subdi ect ries in the /kernel Directory

The following describes the types of module subdirecto ies contained in the /kernel, /usr/kernel,/platform/'uname -m'/kernel, or /platform/'uname -i'/kernel directories:

- drv evice drivers
- exec Executable file formats
- fs File system types, for example, ups in fs, and proc
- misc Miscellaneous modules (virtual swap)
- scited Scheduling classes (p ocess execution scheduling)
- strood Streams modules (generalized connection between users and device drivers)
- sys System calls (defined interfaces (or applications to use)

The /kernel/drv directory contains all of the device drivers that are used for system boot. The /usr/kernel/drv directory is used for all other device drivers.

Modules are leaded automatically as needed either at boot time or on deroand, if requested by an application. When a module is no longer in use, it might be unloaded on the basis that the memory it uses is needed for another task.

After the boot process is complete, device drivers are loaded when devices, such as type devices, are accessed This process is called autoconfiguration because some kernel driver modules are loaded automatically when needed.

Upon initial or reconfiguration book, the system does a self-test und checks for all devices that are attached.

The advantage of this dynamic kernel arrangement is that the overall size of the kernel is smaller, which makes more efficient use of memory and allows for simpler modification and tuning. Figure 9-5 shows this arrangement.

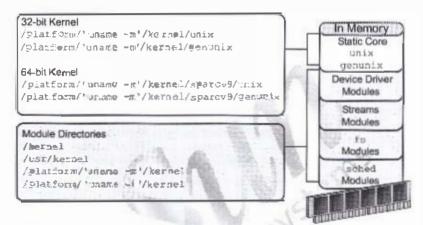


Figure 9-5 The kernel and Modules Loaded in Memory



Note - The aparcy9 CPU is the type of CPU that supports 64-bit processing.

The /etc/system File and kernel Configuration



Caution - The Solaris OE builds the bernel based upon the size of the system (memory, CPUs, and so on). In almost all cases, the performance of the default kernel, that is built is quite adequate to handle most day to day at ivities on the system. Any modifications should be made with extreme caution.

The /etc/system file is the control fite for modifying which modules and parameters are to be loaded by the kernel at boot time. By default, all lines in this file are commented out-

Modifying the heznel's behavior for configuration) requires editing the /etc/gystem file. Altering this file allows you to modify the kernel's treatment of loadable modules as well as to modify kernel parameters for some performance tuning.

The distance program contains a list of default loadable kernel modules that are loaded at boot time. However, you can override this list by modifying the /etc/system file to control which modules, as well as which parameters, are loaded.

All changes to this file take effect after a reboot.

The /etc/system file can explicitly control:

- The search path for default kernel modules to be loaded at boot time
- The root file system type and device
- The modules that are excluded from loading automatically at boot time
- The modules to be forcibly loaded at boot time, rather that at first across
- The new values to override the default kernel parameter values



Note - Command fines must be 80 characters or less in length, and comment lines must begin with an asterisk (*) and end with a newline character.

The /eta/system file is divided into five distinct sections:

· moddig

Sets the search path for default loadable Nexuel modules. You can list together multiple directories to search, delimited either by blank spaces or colons. If the module is not found in the first directory, the second directory is searched, and so on.

root, device and root file system configuration:
 Sets the root file system type to the listed value. The default is zootfs:ufs.

Sets the root device. The default is the physical path name of the device on which the boot program resides. The physical path name is platform dependent and configuration dependent. The following is an example path:

rootdev:/sbus61.f8000000/esp60.800000/sd83.0:a

exclude:

Does not allow the loadable kernel modules to be loaded during kernel initialization, for example:

evalude: sys/ahmays

• fercelead

Forces the kernel modules to be loaded during kernel initialization, for example:

forceload: dry/vo

The default action is to load a kernel module automatically when its services are first accessed during runtime by a user or an application.

Changes kernel parameters to modify the operation of the system, for example:

set maxusers=40

Editing the /etc/system File

Before you edit the /etc/system file, you should make a backup copy. If you enter incorrect values in this file, the system might not be able to book.

The following example shows how to copy the original /etc/system file to a backup file and then edit the /etc/system file.

op /etc/system /etc/system.orig

vi /etc/system

If a boot process fails because of an unusable /etc/system file, issue the interactive boot command: hoot —a. When you are requested to enter the name of the system file, type in the name of your backup system file, or, alternatively, enter /dev/null for a null configuration file.

The init Phase

The final phase of the boot process is the init phase. During this phase, the init daemon starts the run control (rc) scripts that start other processes. The init daemon is a general process spawner. Its primary role is to create processes from information stored in the file /etc/inittab.

The limit daemon executes system star up (no) scripts that, in turn, execute a series of other scripts.

After the init phase comPletes successfully, the default behavior is to display the system command-line login prompt of the GUI login window.

The /etc/inittabFile

When you boot a system or change run levels with the init or shoutdown command, the init daemon stops process, starts processes, or does both by reading information from the /et@/inittan file.

The initial file defines three important items for the init process:

- The system's default run level
- What actions to take when the system enters a new run level
- What processes to start, monitor, or restart if terminated

Each line entry in the /etc/inittab file contains the following four fields:

id:rstate:action:process

Figure 9-b shows an inittab entry.

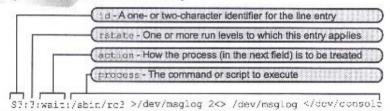


Figure 9-6 An /eto/. Ini ttab File Entry



Note — Message output from so scripts is directed to the /dev/ssglog file. Prior to the Solaris 8 OE, all of these messages were written to the /dev/console file. The /dev/msglog file is used for message output collection from system startup or backgroun applications.

Table 9-2 shows an explanation for each keyword.

Table 9-2 The action Field Keywords

Keyword	Explanation
initdefault	Identifies the default run level. Road when the init process is initially invoked. Used by the init process to determine which run level to enter initially. The default is run level 3.
sysinit	Executes the process before the init process tries to access the coasole (for example, the console login prompt). The init process waits for completion of the process before it continues to read the initial file.
wait	Starts a process and waits for it to complete before moving to the next entry that contains the same run level.
respawn	If the process dies, the init process restarts it. If the process does not exist, the init process starts it and continues resting the initials file. If the process does exist, no action is required, and the init process continues reading the initials file.
powerfail	Executes the process only if the init process receives a power fail signal.



Caution — If the retate field is empty and the initial state line is used, the retate field is interpreted as 0125456, and the init process enters run level 6 as the default. This causes the system to reboot continuously.



Note -1 formation about additional action keywords is available in the inittab man page.

The following is an example of a default /et/c/inittab file.

```
ap::syminit:/shin/actepush -f /etc/iu.ap
ap://sysinit:/sbin/seconfig -f /etc/seck2@ath
is:syminit:/sbin/rdS/syminit/>/dev/magleg/2<>/der/magleg/</der/console
is:3:initdefault:
pd:s1234:powerfail:/usr/sbin/shutdown -y -i5 -g0 >/dev/paglog
2<>/dev/msglog
ss:s:wait:/sbin/rcs
                            >/dev/magieg 2<>/dev/magleg </dev/consele
s0:0:wait:/sbin/rc0
                            >/dev/msglog 2<>/dev/msglog </dev/censele
s1:1:respawn:/sbin/rol
                            >/detr/msgleg 2<>/dev/msglog </dev/censele
s2:23:wait:/abin/rc2
                            >/dev/msglog 2<>/dev/msglog </dev/consele
s3:3:wait:/sbin/rc3
                            >/dev/msglog 2<>/dev/msglog </dev/console
                            >/dev/mmglcg 2<>/dev/mmgleg </dev/console
s5:5:wait:/sbin/rc5
s6:6:30ait:/sbin/rc6
                            >/dev/msglog 2<>/dev/msglog </dev/consele
fw:0:wait:/sbin/uadmir. 2 0 >/dev/msglog 2<>/dev/msglog </dev/console</pre>
of:5:wait:/sbin/uadrin 2 & >/dev/msglog 2<>/dev/msglog </dev/conaple
rb:6:wait:/sbin/uadmin 2 1 >/der//msglog 2<>/dev/msglog </dev/console
sc:234:respawn:/usr/lib/saf/sac -t 300
co:234:respawn:/usr/lib/saf/ttymon -c -h -p "'uname -n' console login: "
-T sum -d /dev/censele -1 console -m idterm, ttcompat/
```



The following describes each of the lines in the initials file in order:

- 1. Initializes the streams modules
- 2. Configures the socket transport providers
- 3. Initializes the file systems
- 4. Defines the default run level
- 5. Describes a power fail shutdown
- 6. Defines single-user mode
- 7. Defines run level 0
- 8. Defines run level 1
- 9. Defines run level 2
- 10. Delines run level 3
- 11. Oefines run level 5
- 12. Petines run level 6.
- 13. Defines the transition to firmware
- 14. Defines the transition to power off
- 15. Defines the transition to reboot
- 16. Initializes the service access controller
- 17. Initializes the tLymon port monitor, which places a command-line login prompt to the console

The init Process

Figure 9-7 shows the process of bringing a system to the default run level 3.

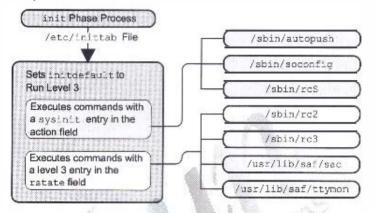


Figure 9-7 The init Process

The init process reads the /etc/inittab file to do the following:

- Identify the initdefault entry, which defines the default run level, 3.
- 2. Execute any process entries that have syminit in the action field so that any special initialization can take place before users log in. This includes the execution of spin/rcs, which mounts and checks the / (root), /usr, /var, and /var/acm file systems.
- Execute any process entries that have 3 in the retate field and an appropriate keyword in the action field, which match the default run level, 3.

The commands executed at this run level include:

- /usr/sbin/shutdown The init process runs the shutdown command only if the system has received a power fail signal.
- /sbin/xc2 Starts the system daemons, bringing the system up into run level 2 (multiuser mode).
- /sbin/ro3 Starts NFS and other network resource servers for run level 3.

- /usr/lib/saf/sac Starts the port monitors for devices, such as ASCII terminals and moderns.
- /usr/lib/saf/ttywon- Starts the ttywon process that
 munitors the console for login requests. The default
 terminal_type on all systems as listed in the /etc/inittab
 file is sun.



Controlling Boot Processes

The Solaris OE provides a series of run control (re) scripts to stop and start processes typically associated with run levels.

The /sbin Directory

Each run level has an associated ro script located in the /slain directory. Figure 9-8 shows the ro scripts associated with each run level in the /slain directory and their inode numbers.

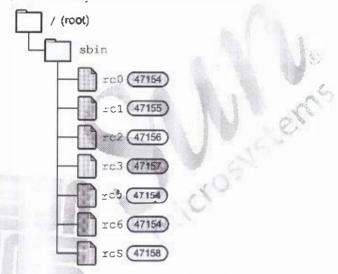


Figure 9-8 The /soin Directory With Inode Numbers

The ro scripts are executed by the init process to set up variables, tost conditions, and make calls to other scripts that start and stop processes for that run level.

The re-scripts re0, re5, and re6 are hard-linked to each other. Notice each script is assigned the same inode number.

The following is an example of the hard links:

The Solaris OE provides the same series of no scripts in the /etc directory for backward compatibility. These scripts are symbolic link files to the no scripts in the /skin directory.

The following example shows this connection:

```
# cd /etc
# ls -1 rc?
                                                 11 Feb 22 14:19 rc0 -> ../sbin/rc0
11 Feb 22 14:19 rc1 -> ../sbin/rc1
11 Feb 22 14:19 rc2 -> ./sbin/rc2
11 Feb 22 14:19 rc3 -> ../sbin/rc2
                1 root.
1:wxrwxrwx
                               reet
               1 geot
INVERTORING.
                               reet
Irwxrwxrwx 1 roct
                               reet
lrwxrwxrwx
                1 rect
                               root
TWENTER THE
                1 reca
                               roct
                                                  11 Feb 22 14:19 rc5 -> ../sbin/rc5
                 1 rect
                                                 11 Feb 22 $4:19 re6 -> ../sbin/re6
LESCORES X
                               rest
                                                 11 Feb 22 14:13 rc5 > ../sbin/rc5
LINCEDOWN 1 root
                               root
```

lable 9-3 summarizes the tasks performed by each of the /sbin ro scripts.

Table 9-3 Run Control Scripts and Their Functions

re Script	Function
/sbin/rc0	Runs the /etc/rc0.d/K* scripts and then the /etc/rc0.d/S* scripts to perform the following tasks: • Steps system services d daemons
	Terminates all nurving processes
	Unmounts all file systems
	Startscripts should only perform fast system cleanup functio #.
/sbin/rcl	Runs the /etc/rc1.d/5* scripts to perform the following tasks: • Stops system services and daemens
	Terminates all running user processe
	Unmounts all remote file systems
	Mounts all local file systems if the previous run level was S

Table 9-3 Run Control Scripts and Their Functions (Continued)

re Script	Function
/sbin/rc2	Runs the/etc/rc2.d/K* scripts and then the /etc/rc2.d/S* scripts to perform the following tasks: • Mounts all local (le systems if the previous can level) was S
	Removes any files and subdirectories in the /tmp directory
	Configures system accounting
	Configures the default router
	Starts most of the system daemons
/sbin/rc3	Runs the /etc/rc3.d/K* scripts and then the /etc/rc3.d/S* scripts to perform the following tasks: Cleans up the /etc/dfs/s/paretab @c
	• Shares all resources listed in the /etc/dfs/dfst.ab file
	Starts the rifes and mount dicommands
	Note: Kiscripts are not normally present in the /ete/mc3 d directory, although if they were present, they would be run.
/sbin/rc5 /sbin/rc6	Runs the /etc/rc0.d/x* scripts and then the /etc/rc0.d/s* scripts to perform the following tasks: • Stops system services and daemons
	1erminates all running processes
	Unmounts all file systems
	Starts scripts that should only perform fast system cleanup functions
/ebin/res	Runs the /etc/rcs.d scripts to bring up the system to run level S: • Establishes a minimal network
	 Mounts the /usr, /var, and /var/adm directuries if they are separate file systems.
	Sets the system name
	Checks the / (root) and /usr file systems
	Mounts pseudo file systems (/proc.and /dev/fd)
	Rebuilds the device entries for reconfiguration boo s
	Mounts other file systems that are required in single-user mode

The /etc/rc#.dDirectories

The /etc/re#.d directories contain additional scripts that start and stop system processes for that run level.

Figure 9-9 shows an example of /etc/ro#.d directories.

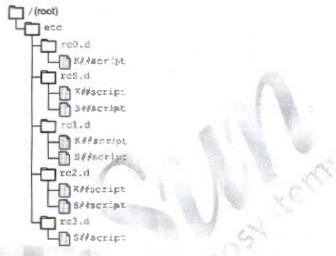


Figure 9-9 The /etc/let.d Directories

For example, #e0s/rc2.d contains scripts to start and stop processes for rulevel 2. The following output shows a partial list of these scripts.

ls -1 /etg/rc2.d

1960 100 000000	1000	The second second second						
-rwxrr	6	root	sys	344	Jun	19	18:56	K06mipagent
-11/1XXX	6	rest	sys	404	ហ្គារ	19	17:27	K07srmpdx
-I	6	root	sys	2723	Jur.	19	17:00	K28nfs.server
-TYPOT I	2	reot	sys	1597	J:u:	19	17:00	520sysetup
I	2	root.	sys	989	Jun	19	17:12	S2lperf
-Pare-xe-X	2	Yeet	other	1995	Jwn	25	00:09	830ayaic.net

Start Run Control Scripts

The /eto/rr*.d start scripts are always run in the sort order shown by the 1s command. The files that begin with 5 are run to start a system process. These scripts are called by the appropriate /sbin/rc# and this script passes the argument "scare" to them if their names do not end in .sh. There are no arguments passed to .sh scripts. These files have names in the form of:

S##name-of-script

For example, the script that starts the line printer (LP) processes is named \$80. m.

Stop Run Control Scripts

The /studiecf.d stop scripts (also referred to as the tall scripts) are always run in the sort order shown by the less command. The files that begin with K are run to stop or kill a system process. These scripts are called by the appropriate /sbin/rc#, and this script passes the argument "stop" to them if their names do not end in .sh.

These files have names in the form of:

K##na.me-ef-script

For example, the script that stops the NFS server processes is called ROBDES, server.



Note - File names that begin with a lowercase k ors are ignored by the init process, and they are not executed. To disable a swipt, rename it with the appropriate loweruse letter.

The /etc/init.d Directory

Run control scripts are located in the /etc/init.d directory.

The files shown in Figure 9-10 are hard-linked to corresponding numcontrol scripts in the /etc/re#.d directories.

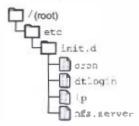


Figure 9-10 The /etc/init.d Directory

The run control script /etc/init.d/cron is high-linked to the corresponding run control script /etc/fc2.d/\$75eron, as shown by the la commands:

The benefit of having individual scripts for each run level is that you can run scripts in the */etc/init.d directory individually as the root user.

You can stop a process or start a process without changing the system's run level.

For example, to stop and restart the LP print services, run the following scripts with a scop or start argument:

- # /etc/init.d/lp stop
- # /etc/init.d/lp start

Creating New Run Control Scripts

You can create new scripts to start and stop additional processes or services to customize a system.

For example, to eliminate the requirement for a manual start of a database server, you could create a script to start the database server automatically after the appropriate network services have started.

You could then create another script to terminate this service and shut down the database server before the network services are stopped.

To add run control scripts to start and stop a service, create the script in the /etc/init.ddirectory and create links in the appropriate /etc/ruf, ddirectory for the run level in which the service is to be started and stopped.

Refer to the README file in each /etc/rc#.d directory for more information on run control scripts.

The following procedure describes how to add a nun control script:

- Create the script in the /etc/init. d directory.
- # vi /etc/init.d/filename
- f chmod 744 /etc/init.d/filename
- # chgrp eys /etc/init.d/filename
 - 2. Create links to the appropriate /etc/init. d directory:
- # cd /etc/init.d
- # ln filename /etc/rc#.d/S##filename
- # 1n filename /etc/rc#.d/K##filename
 - Use the is command to verify that the script has links in the appropriate directories.
- # ls -li /etc/init.d/filename
- # ls -li /etc/rc#.d/S##filename
- # ls -li /etc/rc#.d/K##filename
 - 4. Test the filename by performing the following commands:
- # /etc/init.d/filename start

Figure 9-11 shows the run-level transitions that occur during the process of a system bootup or shutdown.

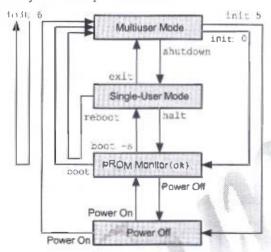


Figure 9-11 Run-Level Transitions



Note — The hai trand report commands shown in Figure 9-11 do not process the initial file as the init and shutdown commands do. The init and shutdown commands are the preferred methods for transitioning between run states.

Performing System Shutdown Procedures

You can shut down the Solaris of to perform administration tasks or maintenance activities if you are anticipating a power outage or if you next to move the system to a new location.

The Selaris OE requires a clean and orderly shutdown, which stops processes, writes data in memory to disks, and unmounts file systems.

•f course, the type of work you need to do while the system is shut down determines how the system is shut down and which command you use.

The following describes the different types of system shutdowns.

- Shut down the system to single-user-mode
- Shut down the system to stop the Solaris OE, and display the ekprompt
- Shut down the salem and turn off power
- Shut down the system and automatically reboot to multiuser mode.

The commands are lable to the root user for Jung these types of system shutdown procedures include:

- /sbin/init (using run levels 5, 0, 1, 5, or 6)
- /usr/sbin/shutdown(using run levels S, 0, 1, 3, or 6)
- /usr/sbin/halt
- /usr/sbin/reboot
- /usr/sbin/poweroff



Note — The init command accepts more arguments than those listed here. These arguments are not listed here because they are outside of the topic of system shutdown procedures.

The /usr/sbin/init Command

You use the init command to shut down, power off, or reboot a system in a clean and orderly manner. It executes the red kill scripts. However, this command does not warn logged-in users that the system is being shut down, and there is no grace period.

To shut down the system to single-user mode, use either run level Set 1.

init 8

To shut down the system to stop the Solaris OE and display the ole primpt, perform the command:

i init 0

To shut down the system and turn its power off, perform the command:

indt 5

To shut down the system and then reboot to multiuser mode, perform the command:

init 6

The /usr/sbin/shutdown Command

The shr:tdown command is a script that invokes the init daemon to shut flown, power off, or reboot the system. It executes the xc0 kill scripts to shut down processes and applications gracefully. But whike the init command, the shutdown command does the following:

- Notifier all logged in users that the system is being shut down
- Delays the shutdown for 60 seconds by default
- Enables you to include an optional descriptive message to inform your users of what will transpire

The command format for the shutdown command is:

shutdown -y -g grace-period -1 init-state optional message

The -y option pre-answers the final shotdown continuation question so that the command runs without your intervention.

The -g grace-periodallows you to change the number of seconds from the 60-second default.

The -t init-state specifies the run-level that the init process is to attain. By default, system state Sis used.



Note — If the shirtdown command displays the error message:
"shurdown: 'i' — unknown flag," it indicates that the shell has located and executed the /wsr/ucb/shurdown command. Reissue the command using its full path (for example, /usr/sbin/shutdown), or set the FATH variable to ensure /usr/sbin comes before /usr/ucb.

To shut down the system to single-user mode, enter the shutdown command without options.

shutdown

To shut down the system to stop the Solaris OE, and display the ok prompt, perform the command:

shutdown -10

To shut down the system and turn off its power automatically, perform the command:

shutdown -15

To shut down the system and then reboot to multiuser mode, perform the command:

shutdown -16

The -i option can be used with other command options. For example, to shut down the system and then reboot to multiuser mode, answer yes to the questions presented, provide a grace period of two minutes, and provide a message to the users, perform the command:

shutdown -y -g120 -i6 "The system is being rebooted"

The /usr/sbin/halt Command

The halt command performs an immediate system shutdown. It does not execute the re0 kill scripts. It does not notify logged-in users, and there is no grace period.

To shut down the system, stop the Solaris OE, and display the ok prompt, perform the command:

halt

The /usr/sbin/poweroff Command

The presence of command performs an irrunediate shutdown. It does not execute the roll kill scripts. It does not notify logged-in users, and there is no grace period.

To shut down the system and turn off its power, perform the command:

poweroff

The /usr/sbin/reboot Command

The respect command performs an immediate shutdown and reinitialization, bringing the system to run level 3 by default. The report command differs from the inity 6 command because it does not execute the Ecc kill scripts.

To short down the system and then reboot to multiuser mode, perform the respect; command without options:

reboot.

Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1. This version of the lab provides the least amount of guidance. Each bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab provides more guidance. Although each step describes what you should do, you must determine the commands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because each step provides exactly what you should input to the system. This level also includes the task solutions for all three levels.



Exercise: Controlling the Boot Process (Level 1)

In this exercise, you create a new startup script, make changes in the /eto/system file, and observe their effects.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed.

Your instructor should provide you with instructions on how to obtain a script called "banner" that will be used during this exercise.

Tasks

Complete the following tasks:

 In the /ctc/r=2.d directory, create a thard link to the /etc/init.d/banner file, called \$225anner. In the /etc/rcs.d directory, create a hard link to the /etc/init.d/banner file called K995anner.

(Steps 1-5 in the Level 2 lab)

Reboot the system and verify that S22tanner runs. Shut down the system to run level S, and verify that K99banner runs, Change back to run level 3. Make a backup copy of the /etc/system file. Check if any instances of the at defer are loaded. Modify the /etc/system file to force-load the st. driver. Reboot the system, and verify that st driver instances are loaded.

(Steps 6-10 in the Level 2 lab)

 Edit the /etc/system file to exclude the boot disk driver for your system (either dad or so). Shut down the system to run level 0, and attempt to boot it. Make note of what happens. Interactively boot your system, and return it to an operational state.

(Steps II-I4 in the Level 2 lab)

Exercise: Controlling the Boot Process (Level 2)

In this exercise, you create a new startup script, make changes in the /etc/system file, and observe their effects.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed.

Your instructor should provide you with instructions on how to obtain a script called pattner that will be used during this exercise.

Task Summary

In this exercise, you accomplish the following:

- In the /etc/rc2.d directory, create a hard link to the /etc/init.d/banner file, called \$22banner. In the /etc/rms.d directory, create a hard link to the /etc/init.d/banner file called \$32banner.
- Reboot the system, and verify that \$22banner runs. Shut down the system to run level 5, and viffy that \$99banner runs. Change back to run level 3. Make a backup copy of the /etc/system file. Check if any instances of the sit driver are loaded. Modify the /etc/system file to forge-load the sit driver. Reboot the system, and verify that sit driver instances are loaded.
 - Edit the /etc/systemfile to exclude the boot disk driver for your system (either dad or sd). Shut down the system to run level 0, and altempt to boot it. Make note of what happens. Boot the system using the -a option of the boot command. Use your backup of the /etc/system file as required Replace the /etc/system file with your backup when finished, and reboot the system.

Tasks

Complete the following steps:

- Log in as the root user, and open a terminal window. Change the directory to /etc/irit.d. Make sure that the barrier script your instructor provided you is present and executable.
- 2. Verify that the script runs with both the start and stop arguments.
- Change the directory to /etc/zc2.d Create a hard link called SZZbanner that points to the same data as the /etc/init..d/banner file.
- Change the directory to the /etc/ros.ādirectory. Create a hard link called K99 sermer that points to the same data as the /etc/ir/it.ā/banner file.
- Reboot the system, and watch for the output of the script you just installed.
 - Docs the startup message from \$22hanner appear?
- 6. Log in as the root user, and open a terminal window. Use the init command to change to run level S.
 - Does the shutdown message from K995armer appear?
- 7. Type the password for the root user to log in at the command line.

 Change to run level 3.
- 8. Log in as the root user ind open a terminal window. Change the directory to leto.
- Make a backup copy of the /etc/system file, and name the backup file yetem.crig.
- 10. If your system uses a SCSI tape device, perform the following:
 - Log in as the root user, and open a terminal window. Use the proconf command to list instances of the st driver currently londed.
 - How marry instances are reported?
 - Edit the /etc/systemfile so that it includes the following line: torcelosal: dry/st
 - Then reboot the system.
 - Log in as zoot, and open a terminal window. Again list includes of the still driver currently loaded.
 - How many instances are reported?

11. Edit the /etc/syst.so file so that it excludes the main disk driver for your system.

On systems using SCSI disks, add the following:

explude: drv/sd

On systems using IDE disks, add the following:

exclude: drv/dad

 Shut down the system to run level 0, and then attempt to boot it again.

What happened?

13. Use the boot —a command to boot the system, and supply the name of your backup file called etc/system.orig (note there is not a leading sloth to the etc). Press the Return Key to accept the default values for all other boot parameters. For example:

ok boot -a

Enter filename [kernel/spacev9/unix]: @sturn>
Enter default directory for minutes (Volations...): @sturn>
Name of system the letc/system): atc/system.orig
root filesystem type (uis): @sturn>
Enter physical name of root device [/...]: @sturn>

14. Log in as the root user, and open a terminal window. Copy the /etc/system.orig file to the /etc/systemfile. Reboot this system.

Exercise: Controlling the Boot Process (Level 3)

In this exercise, you create a new startup script, make changes in the /etc/system file, and observe their effects.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed.

Your instructor should provide you with instructions on how to obtain a script called banner that will be used during this exercise.

Task Summary

In this exercise, you accomplish the following:

- In the /erc/rc2.d directory, create a hard link to the /etc/init.d/banner file, called \$22banner. In the /etc/rc8.d clirectory, create a hard link to the /etc/init.d/manner file called K99manner.
- Reboot the system, and verify that \$225anner runs. Shut down the
 system to run level \$5, and verify that \$225anner runs. Change back
 to run level \$3. Make a backup copy of the /etc/systemfile. Check if
 any instances of the ut driver are loaded. Modify the /etc/system
 file to force-load the st driver. Reboot the system, and verify that st
 driver instances are loaded.
- Edit the /e@o/system file to exclude the book disk driver for your system (either dad or ad). Shut down the system to run level 0, and attempt to boot it. Make note of what happens. Boot the system using the -o option of the boot command. Use your backup of the /eco/system file as required. Replace the /eco/system file with your backup when finished, and reboot the system.

Tasks and Solutions

Complete the following steps:

- Log in as the root user, and open a terminal window. Change the directory to /eto/init. a. Make sure that the manner script your instructor provided you is present and executable.
- # cd /etc/init.d
- # ls -1 banner
- # chunod 744 benner
 - Make the banner script executable, and verify that it runs with both the start and atop arguments.
- # ./bapper start
- # ./banner stop
 - Change the directory to the /etc/zc2.cdirectory. Create a hard link called \$22barner that points to the same data as the /etc/init.d/barner file.
- # cd /etc/rc2.d
- # ln /etc/init.d/benner 822benner
 - Change the directory to the /etc/ros.d directory. Create ahard link called R99banner that points to the same data as the /etc/init.d/banner file.
- # cd /etc/rcs.d
- # ln /etc/init.d/banner K99 banner
 - Reboot the system, and watch for the output of the script you just installed.
- # init 6

Does the startup message from S22benner appear?

Yes

- Log in as the root use; and open a terminal window. Use the init command to change to run level S.
- f init S

Does the shutdown message from K99banner appear?

Yes.

- Type the password for the root user to log in at the command line. Change to run level 3.
- # init 3

Log in as the root user, and open a terminal window. Change the directory to /etc.

cd /etc

 Make a backup copy of the /eto/systemfile, and name the backup file system.orig.

CP system.orig

- 10. If your system uses a SCSI tape device, perform the following:
 - Log in as the root user, and open a terminal window. Use the priconf command to list instances of the st driver currently loaded.

prtconf | grep "st, instance"

How many instances are reported?

Noune

b. Edit the /etc/system file so that it includes the following line: forceletal: drv/st

Then rebrot the system.

init 6

 Ung in as root, and open a terminal window. Again list instances of the at driver currently loaded.

ortcomf | grep "st, instance"

How many instances are regerted?

The number varies depending on how many SCSI controllers a represent. You should see instances I through 6 for a system with one controller.

 Edit the /ctc/aystem file so that it excludes the main disk driver for your system.

On systems using SCSt disks, add the following:

exclude: árv/sd

On systems using IDE disks, add the following:

extlude: dry/dad

- Shut down the system to run level 0, and then attempt to boot it again.
- # emitdown -y -i0 -g0 (shutdown messages)
- ek boot

What happened?

The system is numble to boot. Excluding this driver prevents you from using the boot disk so long as you use the same /eto/system file. You must boot using the -e option to be able to supply an alternative file for the /eto/system file.

13. Use the boot —a command to boot the system, and supply the name of your backup file called etc/system, orig (Note there is not a leading slash to the etc.). Press Return to accept the default values for all other boot parameters. For example:

ek boot -s

Enter filename [kernel/sparcy9/unix]; <Return>
Enter default directory for modules [/platform...]; <Return>
Kame of system file [stc/system]; otc/system.orig
rmot filesystem type [his]; <Return>
Enter physical name of root device [/...]; <Return>

- 14. Log in as the root user and open a terminal window. Copy the /etc/system.or19 file to the /etc/system file. Reboot the system.
- # cd /etc
- # cp system.orig system
- # init 6

Exercise Summary



Discussion – Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercise.

- Experiences
- Interpretations
- Conclusions
- Applications



Performing User Administration

Objectives

Upon completion of this module, you should be able to:

- Describe user administration fundamentals
- Manage user accounts
- Manage initialization files

The following course map shows how this module fits into the current instructional goal.

Performing User and Security Administration

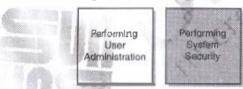


Figure 10-1 Course Map

Introducing User Administration

An important system administration task is setting up user accounts for each user who requires system access. Each user needs a unique account name, a user identification (UID) number, a home directory, and a login shell. You also have to determine which groups a user may access.

Main Components of a User Account

The following is a first of the main components of a user account:

- User name A unique name that a user enters to log in to a system.
 The user name is also called the login name.
- Password A combination of six to eight letters, mambers, or special
 characters that a user enters with the login name to gain access to a
 system.
- UTD number A user account's unique runtimical identification within the system.
- Group identification (GID) number A unique numerical identification of the group to which the user belongs.



Note - You fan add a user to predefined groups listed in the /etc/group file.

- Comment Origination that identifies the user. A comment generally colliains the full name of the user and optional information, such as a phone number or a lucation.
- User's home directory A directory into which the user is placed after login. The directory is provided to the user to store and create files.
- User's login shell The user's work environment is set up by the initialization files that are defined by the user's login shell.
- Password aging An optional feature to require users to change their passwords on a regular basis.

System Files That Store User Account Information

The SolarisTM Operating Environment (Solaris OE) stores user account and group entry information in the following system files:

- /etc/pagewd
- /etc/shadow
- /etc/group

Authorized system users have login account entries in the /etc/passwf file.

The /etc/stractor file is a separate file that contains the encrypted passwords. To further control user passwords, you can enforce password aging. This information is also maintained in the /etc/shadow file.

The /etc/group file defines the default system group entries. You use this file to cruste new group entries or modify existing group entries on the system.

The /etc/passwd File

Due to the critical nature of the /ecc/passwd file, you should refrain from editing this file directly. Instead, you should use the Solaris⁷⁶¹
Management Console or command-line tools to maintain the file.

The following is an example of an /eto/passwil file that contains the default system account entries.

```
root:x:0:1:Super-User:/:/sbin/sh
demon:x:1:1:0::
bin:x:2:2::/32/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
ls:x:71:6:Line Printer Admin:/usr/spool/ls:
urcp:x:5:5:uucp Admin:/usr/lib/uucp:
nucp:x:5:5:uucp Admin:/var/spool/uucppublie:/usr/lib/uucp/uucico
swsp:x:25:25:5=dMail Message Submission Program:/:
listen:x:37:4:Network Admin:/usr/net/nls:
ncMody:x:60001:80001:Nebody:/:
noaccess:x:60002:40002:No Access User:/:
nebody4:x:65534:65534:8ur.OS 4.x Nobudy:/:
```

Each entry in the /eto/passed file contains seven fields. A colon separates each field. The following is the format for an entry:

loginID:x:UID:GID:comment:home_directory:login_shell

Table 10-1 defines the requirements for each of the seven fields.

Table 10-1 Helds in the /etc/passed File

Field	Description
loginID	Represents the user's login name. It should be urique to each user. The field should contain a string of no more than eight letters (A-Z, a-z) and numbers (0-9). The first character should be a letter and at least one character should be lowercase.
***	Note – Even though some programs allow a maximum of 32 characters, as well as user names that contain periods (.), underscores (.), and hyphens (.), this practice is not recommended and might cause problems with other programs.
х	Represents a placeholder for the user's encrypted password, which is kept in the /etc/shadow file.
UID	Contains the UID number used by the system to identify the user. UID numbers for users range from 100 to 60000. Values 0 t roug 99 are reserved for system accounts. UID number 60001 is reserved for the nobody account. UID number 60002 is reserved for the noaccess account. While duplicate UID numbers are allowed, they should be avoided unless absolutely required by a program.
	Note - The maximum value for a UID is 2147483647. Flowever, the UIDs over (0000 do not have full utility and are incompatible with some Solaris OE leatures. Avoid using LIDs over 60000 so us to be compatible with earlier versions of the operating environment.

Table 10-1 Fields in the /etc/passod File (Continued)

Field	Description
GID	Contains the GID number used by the system to identify the user's primary group. GID numbers for users range from 100 to 60000. (Those between 0 and 99 are reserved for system accounts.)
comment	Typically contains the user's full name.
home_directory	Contains the full path name to the user's home directory.
login_shell	Defines the u er's login shell. There are six possible login shells in the Solaris OE: the Bourne shell, the Korn hell, the C shell, the Z shell, the BASt I shell, and the TC shell.

Table 10-2 shows the default system account data for entries in the /etc/massod file.

Table 10-2 Default System Account Entries

User Name	User ID	Description
root	0	The root account that has access to the entire system. If has at most novestiletions and overrides all other logins, protections, and permissions.
daemon	1	The system daemon account that is associated with routine system tasks.
bin	2	The administrative daemon account that is associated with running system binary files.
sys	3	The administrative daemon account that is associated with system logging or updating files in temporary directories.
adm	4	The administrative daemon account that is associated with system logging.
lp.	71	The line printer (1p) daemon account.
uucp	5	The daemon account associated with UNIX®-to-UNIX Copy Prolecol (UUCP) functions.
nuucp	6	The account that is used by remote systems to log in to the host and start file transfers.

Table 10-2 Default System Account Entries (Continued)

User Name	User ID	Description
smmsp	25	The sendmail message submission daemon account.
listen	37	The network listener daemon account.
nobody	60001	The anonymous user account that is assigned by a Network File System (NFS) server when an unauthorized root user makes a request. The noioody user account is assigned to software processes that do not need any special permissions.
noscess	60002	The account assigned to a user or a process that needs access to a system through some application instead of through a system login procedure.
nobody4	65534	The anonymous user account that is the SunOS™ 4.0 or 4.1 software version of the nobody account



Note - The nubody accounting cures NFS gesources. When a user is logged in as root on an NFS client and altempts to access a remote file resource, the UID number changes from 0 to the UID of nobody (60001)

The /etc/shadowFile

Due to the critical nature of the /etc/shadowfile, you should refrom from editing it directly. Instead, maintain the fields of the file by using the Solaris Management Console or command-line looks. Only the root user can read the /etc/shadow file.

The following is an example /etc/shadow file that contains initial system account entries.

```
root: 5RiJS.yvdG8kU:6445; :::::
demmnNP:6445;; ::::
sys:NP:6445;; ::::
adm:NP:6445; :::::
1p:NP:6445; :::::
twcp:NP:6445; :::::
swsp:NP:6445; :::::
swsp:NP:6445; :::::
```

Each entry in the /etc/shadow file contains nine fields. A colon separates each field. The ninth field is r served for future use and is not currently use.

Following is the format of an entry:

loginID:password: lastchg:min: nex: warn: inactive: expire:

Table 10-3 defines the requirement reach of the eight fields.

Table 10-3 Fields in the /etc/shadow File

Field	Description
loginu	The useg's login came
password	A 13-character encrypted password. The string *LKr indicates a locked actionst, and the string NP indicates no valid password. Passwords must be reconstructed to meet the following requirements: the password must be at least six characters and contain at least two alphabetic characters and at least one numeric or special character. It cannot be the same as the login ID or the reverse of the login ID.
lastchg	The number of days between January 1, 1970, and the last password modification date.
min	The minimum number of days required between password changes.
max	The maximum number of days the password is valid before the user is prompted to enter a new password at login.
warn	The number of days the user is warned before the password expires.
inactive	The number of inactive days allowed for the user before the user's account is locked.

Table 10-3 Fields in the /ecc/scadow file (Continued)

Field	Description
expire	The date (given as number of days since january 1, 1970) when the user account expires. After the date is exceeded, the user can no longer log in.

The /etc/groupFile

Each user belongs to a group that is referred to as the user's primary group. The GID number, located in the user's account entry within the /etc/passwd file, specifies the user's primary group.

Each user can also belong to up to 15 additional groups, known as secondary groups. In the /etc/group file, you can add users to group entries, thus establishing the user's secondary group atfiliations.

The following is an example of the default entries in an /etc/group file:

rest::0:noct

him::2:root,him,desor. sys::2:root,him,sys,Adm adm::4:root,adm.daman uucp::5:root,uarp

mail::6:root tty::7:root,ach lp::8:root,lp.adm muucp::9:root,nuucp staff::10:

daenon:: 12:root, dammon

sysadmin::14: smmp::25:smmp nobody::60001: noaccess::60002: cogroup::65534:

Each line entry in the /ete/group file contains four fields. A colon character separates each field. The following is the format for an entry:

groupname:group-password:GID:username-list

Table 10-4 defines the re-unrements for each of the four fields.

Table 10-4 Fields in the /etc/group File

Field	Description
groupname	Contains the name assigned to the group. Group names contain up to a maximum of eight characters.
group-password	Usually contains an empty field or an asterisk. This is a relic of earlier ver ions of UN X. A group-pas word is a security hole because it might allow an unauthorized user who is not a member of the group but who knows the group password, to enters the group.
	Note - The newgra command thanges a user's primary group association within the shell environment from which it is executed. If this new, active group has a password and the user is not a listed member in that group, the user must enter the pas word before the newgrp command can continue.
GID	Contains the group's GID number. It is unique or the local system and should be unique across the organization. Numbers 0 to 99, 60001, 60002 and 65534 are reserved for system group entries. User defined groups range from 100 to 60000.
username-list	Contains a comma separated list of user names that represent the user's secondary group memberships. By default, each user can belong to a maximum of 15 secondary groups.
	Note - The maximum number of groups is set by the kernel parameter called ngroups_max. You can set this parameter in the /etc/system file to allow for a maximum of 32 groups. Not all applications will be able to reference group memberships greater than 16. NFS is a notable example.

The /etc/default/passwd File

Set values for the following parameters in the /ecc/default/passwd file to control properties for all users' passwords on the system:

- MAXAZEKS Sets the maximum time period (in weeks) that the password is valid.
- MINNTERS Sets the minimum time period before the passord can be changed.
- PASSLENGTH Sets the minimum number of characters for a password. Valid entries are 6, 7, and 8.
- WARNVEEKS Sets the time period prior to a password's expiration to warn the user that the password will expire.



Note - The WARNAEEKS value does not exist by default in the /etc/default/passwd file, but it can be added.

The password aging parameters MAXWEEKS, MINWEEKS, and WARN-JEEKS are default values. If set in the /etc/shadowfile, the parameters in that file override those include /etc/default/passwd file for individual users.

Managing User Accounts

Each of the following sections present two sets of command-line tools for managing user accounts: the command-line tools used in the Solaris OE versions prior to the Solaris OE, and the new set of command-line tools developed for the Solaris 9 OE.

Introducing Command-Line Tools

The Solaris 7 OE and the Solaris 8 OE provide you with command-line tools, defined as follows:

- useradd Adds a new user account on the local system
- userned Modifies a user's account on the local system
- userdel Deletes a user's account from the local system
- groupedd Adds a new group entry to the system
- groupped Modifies a group entry on the system
- groupdel Deletes a group entry from the watern

In addition to these command-line tools, the SoI ris 9 OE has a new set of command-line tools that accomplish the same tasks. If eyere the source and strong commands.

The smiler command enables you to manage one or more users on the system with the following set of subcommands:

- Adds a new user account
- Rodity Modifies a user's account
- 5@et# Deletes a user's account
- Tist Lists one or more user entires



Note – The amuser and sugroup commands are the command-line interface equivalent to the Solaris Management Console range of operation, and allow you to perform Solaris Management Console actions in scripts. Therefore, the sameer and sugroup commands have numerous subcommants and options designed to function across domains and multiple systems. This module describes only the basic commands.

The amproup command enables you to manage one or more groups on the system with the following set of subcommands:

- add Adds a new group entry
- modify Modifies a group entry
- delete Deletes a group entry
- list Lists one or more group entries

Any subcommand to add, modify, list, or delete users with the smaller and amgroup commands requires authentication with the Soloris Management Console server and requires the initialization of the Solaris Management Console. For example, the following is the command format for the smaller command:

/usr/sacm/bin/smuser subcommand [auth_ergs] - [subcommand_args]

The authorization arguments are all optional. However, if you do not specify the authorization argument, the system might prompt you for additional information, such as a password for authentication purposes.

The -- option separates the subcommand-specific options from the authorization arguments. The -- option must be entered even if an authorization argument is not specified because it must precede the subcommand arguments.

The subcommand arguments are quite numerous. For a complete listing of the subcommands, refer to the smuser man page. It is important to note that descriptions and other arguments that contain white space must be enclosed in double ou tation marks.

Creating a User Account

Use the userac6 or smuser add command to add new user accounts to the local system. These commands add an enir for a new user into the /etc/passwd and /etc/shadow files.

These commands also automatically copy a 1 the initialization files from the /etc/skel directory to the user's new home directory.

The useradd Command Format and Options

The following is the command format for the useradd commund:

```
userado [ -u uid ][ -g gió ][ -G giá [,gió,...]]
[ -d dir ][ -n [[ -s sheil ][ -c commant ] logimume
```

Table 10-5 shows the options for the userand command

Table 10-5 Options for the us equal Command

Option	Definition
-∵ uid	Sets the UID number for the new user
-g <i>giđ</i>	Defines the new user's primary group
-© gid	Defines the new user's secondary group memberships
-d dir	Defines the full path name for the user's home directory
-m	Creates the user's home directory if it does not already exist
-s shell	Defines the full path name for the shell program of the user's login shell
-c comment	Specifies any comment, such as the user's full name and location
loginname	Defines the user's login name for the user account
-D	Displays the defaults that are applied to the useradd command

The following example uses the useracia command to create an account for a user named new meet. It assigns 100 as the UID number, adds the user to the group other, creates a home directory in the /export/home directory, and sets /bin/ksh as the login shell for the user account.

weradd -u 100 -g other -d /export/home/cover1 -m -s /bin/heb -c "Regular User Account" newser1

84 blocks

H

User accounts are locked by default when added with the useradel command.

By convention, a user's login name is also the user's home directory name.

You use the passwd command to create a password for the new account.

passwd newserl

New Pasaword: 123pass

Re-enter new Password: 123pass

passwd: Pasaword successfully changes for newser1

The smuser add Command Format and Options

The following is the command format for the smuser add command:

smuser add [auth_args] -- [subcommand args]

Table 10-6 shows some of the most common subcommand arguments for the smuser and command.

Table 10-6 Subcommand Arguments for the sauser add Command

Subcommand Argument	Definition
-c comment	A short description of the login, typically the user's name. This string can be up to 256 characters.
-d directory	Specifies the home directory of the new user and is limited to 1024 characters.
-g group	Specifies the new user's primary group membership.

Table 10-6 Subcommand Arguments for the small add Command (Continued)

Subcommand Argument	Definition
-G group	Specifies the user's secondary group membership.
-n <i>login</i>	Specifies the user's login name.
-s shell	Specifies the full path name of the user's login sholl,
-u uid	Specifies the user ID of the user you want to add. If you do not specify this option, the system assigns the next available unique UID greater than 100.

The following example uses the sauser and command to create an account for a user named newser2. It designates the login name as measure2, assigns the UTD number 500, adds the user to the group other, creates a home directory in the /export/home directory, and sets /bin/ksh as the login shell for the user account.



Note – The $-\kappa$ autohome-Noption to the sauser command adds the user without automounting the user's home directory. See the man page for automount for more information.

/usr/sadm/bin/smuser edd -- -n newuser2 -u 500 -g other -d /export/home/msquser2 -c "Regular User Account 2" -s /bin/ksh -x autohome-N

Authenticating as user: root

Type /? for help, pressing center accepts the default denoted by [] Please enter a string value for: password :: EnterPassword Leading Tool: own.sun.admin.userway.cli.user.UserMgrCli from sys41 Login to sys41 as user root was successful. Download of com.sun.admin.userway.cli.user.UserMgrCli from sys41 was successful.

Users are added without a passwood by default with the snuser command. Use the passwo command to create one.

Passwd newser2

New Password: 123pass

Re-enter new Password: 123pass

passwd: password siledestully changed for newuser2

Modifying a User Account

Use the unermodor smuter modify command to modify a user's login account on the system.

The usermed Command Format and Options

The following is the command format for the userned command:

```
usernoč | -u uid ( -c | ) [ -g gid ] [ -G gid ] , gid . . . ] ]
| -d dir | [ -m | | -s shell | | -c comment ]
[ -1 newlognamo] log(rname
```

In general, the options for the assermed command function the sale as those for the useradd command.

Table 10-7 shows the key options to the usermod command.

Table 10-7 Key Options for the unermod Command

Option	Definition
-0	Allows a UID to be duplicated.
-п.	Moves the user's home directory to the new location specified with the -d option.
-1 newlogname	Changes a user's login name for the specified user account.
-f inactive	Sets the number of inactive days that are allowed on a user account. If the account is not logged in to for the specified number of days, it is locked.
-e expire	Sets an expiration date on the user account. Specifies the date (ord cal yr) on which a user our no longer log in and access the account. After that date, the account is locked.
Loginname	Identifies the user's login name for the current user account.

The following example changes the login name and home directory for newser1 to users.

10-15

usermod -m -d /export/home/usera -l usera newuser1

The snuser modify Command Format and Options

The following is the command format for the sauser modify command:

smuser modify (auth_args] -- [subcommand_args]

In general, the options for the smuser modify command function the same as for the smuser add command. Refer to the smuser (1) Il man page for additional options.

Table 10-8 shows the options for the stuser wocify command.

Table 10-8 Options for the sauser medify Command

Option	Definition
⊸n login	Specifies the user's login name
-N legin	Specifics that usen sneswlogin name

The following comple changes the logic name and home directory for new === 2 to user in.

/usr/sadm/bin/smuser modify -- -n newser2 -N userb -d /export/home/userb

Authenticating as user: root

Type /: for help, pressing <enter> accepts the efault denoted by [] Please enter a string value for: password :: EnterPassword
Loading Tool: com.sum.admin.usermyr.cli.user.UserMgrCli from sys41
Login to sys41 as user root was successful.
Domiload of com.sum.admin.usermyr.cli.user.UserMgrCli from sys41 was successful.

Deleting a User Account

Use the unertial command or shower delete current to delete a user's login account from the system.

The following is the command format for the userdel command:

userdel -r togin

The userdel command also removes the user's home directory and all of its contents if you request it to do so. Use the -r option to remove the user's home directory from the local file system. This directory must exist.

The following emurple reproves the login account for a user named

vserdel usera

To request that both the user's Strount and home directory be nanoved from the system at the same time, perform the command:

userdel -r usera

The smuser delete Command Format and Options

The following is the command innat for the snuser delete command: smuser delete [auth_args] -- [subcommand_args]

The following example removes the user's account from the system:

/usr/sact/bin/smuser defete -- -n userb Authenticating as user: rock

Type /? for help, pressing centers accepts the default denoted by [] Please enter a string value for: password :: EnterPassword
Loading Tool: tom.sun.admin.userMgr.cli.user.UserMgrCli from sys41
Login to sys41 as user root was successful.
Download of com.sun.admin.usermgr.cli.user.UserMgrCli from sys41 was successful.



Note — Unlike the user: iel command, the smuser delete command has no —r equivalent option for deleting the home directory. The user's home directory must be deleted manually.

Creating a Group Entry

As the root user, you create new group entries on the local system by using the group add or sngroup add command. These commands add an entry for the new group into the /etc/group file. Like the smuser command, the sngroup add command uses the same subcommands and authentication arguments derived from the Solaris Management Console.

The groupadd Command Format and Options

The following is the command format for the groupedd command:

groupadd [- 9 gra [-0]] groupname

Table 10-9 shows the options for the grospada command.

Table 10-9 Options for the growers & Command

Option	Description Assigns the GIO number for the new group		
-g gžd			
-o Allows the GID number to be duplicate			

The following example uses the groupadd conurrand to create the new group class on the laws system:

groupald -g 301 class

The smgroup add Command Format and Options

The following is the command format for the singroup add command:

/usr/sadm/bin/engroup subcorrend [auth_args] — [seigneend_args]

lable 10-10 shows the options for the suggestion and command.

Table 10-10 Options for the suggeout and Command

Option	Description
-g gid	Specifies the GID number for the new group
-m group_member	Specifies the new members to add to the group
-n group_name Specifies the name of the new group	

The following example uses the sargroup and command to create a new group called works group with a GlD of 123, and to add users to the group:

/usr/sadm/bin/smgroup add -- -n workgroup -g 123 -m usera Authenticating as users root

Type /? for help, pressing kenters accepts the default denoted by [] Please enter a string value for: <code>Massword</code> :: <code>EnterPassword</code> Loading Tool; com.sun.admin.usermgr.cli.group.UserMgrGroupCli from sys4l Login to sys4l as user root was successful.

Download of com.sun.admin.usermgr.cli.group.UserMgrGroupCli from sys4l was successful.

Modifying a Group Entry

You can use the following commands to modify a group entry:

- The groupmed command
- The smgroup modify command

The groupmod Command Format and Options

The following is the command format for the groupmed command:

groupwid [-g gid [-o |] [-: nama [grouppame

Table 10-11 defines the o tions for the groupped command:.

Table 10-11 Op ions for the groupmed Command

Options	Description .
-g giđ	Specifies the new GID number for the group
-0	Allows the GID number to be duplicated
-n name Specifies the new name for the group	

The following example changes the class account group CID number to $400 \colon$

groupsod -g 400 class

The sagroup modify Command Format and Options

The following is the command format for the angroup modifycommand:

/usr/asdm/bin/smgroup subcommand [suth_ar s] -- [subcommand_args]

Table 10-12 shows the options for the sngroup modify command.

Table 10-12 Options for the angroup modify Command

o ption	Description
-n name	Specifies the name of the group you want to modify
-m new_member	Specifies the new members to add to the group
-N new_group	Specifies the new group name

The following example changes the group workgroup to school group:

if /usr/sadm/bin/swgroup modify -- -n workgroup -N schoolgroup Authenticating as user: reet

Type /? for help, pressing <enter> accepts the default denoted by [] Please enter a string value for: password :: EnterPassword Loading Tools com, sun, admin. usermgr.cli.group.UserMgrGroupCli from sys41 Login to sys41 as user root was successful.

Download of com sun, admin. usermgr pari, group. UserMgrGroupCli from sys41 was successful.

Deleting a Group Entry

Use the groupdel or smaroup delete commands to delete a group entry from the /etc/group file on the system.

The groupdel Command Format

The following is the command format for the groupdel command:

groupdel grouptime

The following example removes the group entry class from the local system:

groupdel class

The smgroup delete Command Format and Options

The following is the command format for the smgroup delete command:

/usr/sadm/bin/sugroup subcommend (suth_srgs) -- (subcommend_args)

You can use the -n group_name option with the smeroup delete command to specify the name of the group you want to delete.

The following example deletes the group entry achoolgroup from the local system:

/ /usr/each/bin/emyrum delete -- -n schoolgroup

Losding Tool: com.sum.udmin.isemmgr.cli.group.UserMyrGroupCli from sys41 Login to 5/541 as user root was successful. Download of com.sum.zdmin.usermgr.cli.group.UserMyrGroupCli from sys41

was successful.

Using the Solaris Management Console Users Tool

The Solaris Management Console Users 1001 is a graphical user interface (GUI) that provides access to Solaris OE system administration tools. You can use it for adding, removing, and modifying user and group entries. The following sections contain a demonstration.

Start the Solaris Management Console by typing suck on the command line or by clicking the SMC icon under the Tools submenu. After the "Welcome to Solaris Management Console" message appears, click This Computer to open the Solaris Management Console window, See Figure 10-2.

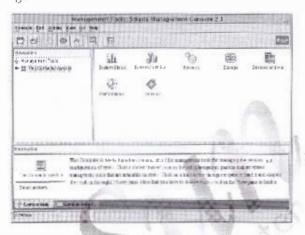


Figure 10-2 Solaris Management Console Window

Adding a User Account

The default method of adding a user account through Solaris Management Console is to add the user account with the user's home directory automounted. The following steps demonstrate how to build a user template that adds the user account with the user's directory under the /exporthone directory.

To add a user account, perform the following steps:

- Click this Computer in the Navigation pane to display the system management tools.
- Click System Configuration to display the fool for setting up a new user acrount.
- Click Users and enter the user name and password to be used for authentication if prompted to do so by Solaris Management Console.
- Double-click User Templates to access the tool to create and manage user templates.
- 5. From the Menu Bar, select Add User Template from the Action list.

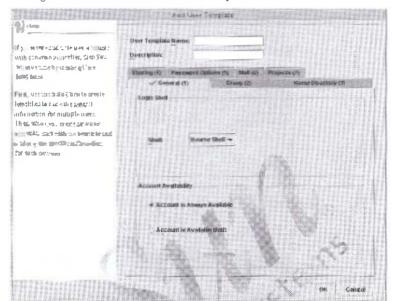


Figure 10-3 shows the Add User Template window.

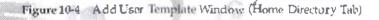
Figure 10-3 Add User Template Window

- Type the name SA239user in the User Template Name field. You can
 provide an optional description if you wish.
- 7. Click the Home Directory tab. Type your syste name in the Home Directory Server field. Uncheck the check box labeled Automatically Mount Home Directory.

Check that better better directory

When the boxe directory as anomalies more to end of the first box directory and the first box directory an

Figure 10-4 shows the Add User Template wandow with the Home Directory Informati in completed.



8. Click OK, and the Solaris Management Console (User Templates) window (Figure 10-5) reappears with the 3a239user template in the View pane.

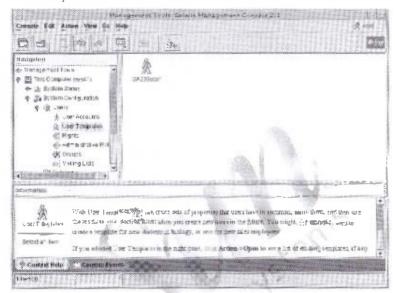


Figure 10-5 Management Tools: Solaris Management Console Window – User Templates

 Click User Accounts from the Navigation pane, and a list of user accounts on the system appears in the View pane. See Figure 10-6.

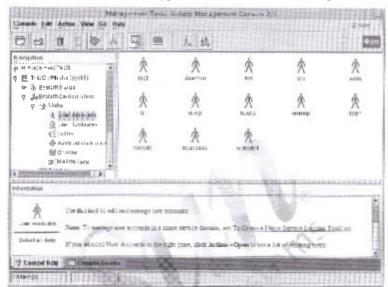


Figure 10-6 Management Tools: Solaris Management Console Window – User Accounts

 From the Menu Bar select Action. Then select Actd User and then select From Template. The Add User From Template window appears. See Figure 10-7.

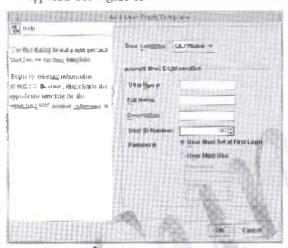


Figure 10-7 Add Ser From Templato Window

Because you only have one template created, it is the default template available from the User Template pull- own list.

- 11. In the field beside User Name, enter the login ID of the user you wish to create. A full name and description are optional.
- 12. Click the button User Must Use and fill in the password and confirmation fields with the password 123 pages.
- Click OK and the Solaris Management Console (User Accounts)
 window reappears with the user account you just created in the
 View pane.

14. Oruhle-dick the user account you just created. The User Properties window appears (Figure 10-8). You can view and modify the properties of that user account.

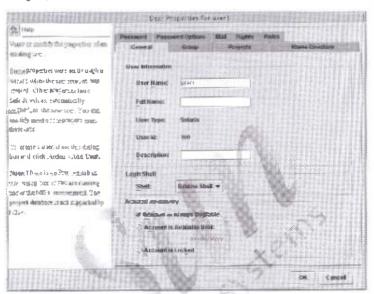


Figure 10-8 User Properties Window

15. Çlick the Group tab

The screen changes to reveal a list of groups. Figure 10-9 shows the information under the Group tab, including the primary group to which the user belongs and a list of available groups.

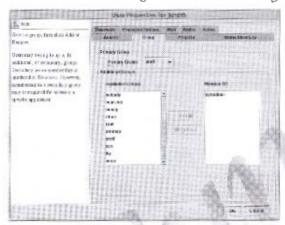


Figure 10-9 User Properties Window - Adding Groups

- You can click a group listed under Available Groups, and then dick Add, and the group moves into the Member Of column.
- 17. Add the groups to which you want the user to belong, and then click OK.

Deleting a User Account

Figure 10-10 shows the initial steps you take to remove a user account from the system.

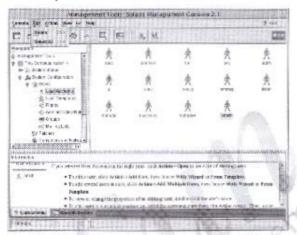


Figure 10-10 Management Tods: Solaris Management Convole Window - Deleting a User Account Window

- 1. Highlight the user account in the User Accounts window.
- 2. From the Menu Bar, click Edit. Select Delete from the Edit menu.

 Figure 10-11 shows the warning window that appears asking you to verify that you want to delete the user account.



Figure 10-11 Warning: Delete User

This window also contains options to remove the user's home directory and to remove the user's mailbox.

Thack the appropriate boxes, and then click Delete. The user account is deleted.

Troubleshooting Login Issues

Some of the most onomon problems you might e counter as a system administrator are user login problems. There are two categories of login problems: login problems when the user logs in at the command line and login problems when the user logs in from the Common Desktop Environment (CDE).

The CDE uses more configuration files, so there are more potential problems associated with logging in from the CDE. When you troubleshoot a login problem, first determine whether you can log in from the command line. Attempt to log in from another system by using either the telnet command or the rlogin command, or click Options from the CDE login panel and select Command Line Logi. If you can log in successfully at the command line, then the problem is with the CDE configuration files. If you cannot log must the command line, then the problem is more serious and involves key configuration files.

Login Problems at the Commend Line

Table 10-13 presents an overview of common login problems that occur when the user logs in at the command line.

Table 10-13 Login Problems at the Command Line

Login Problem	Děscriplión		
Login incorrect	This message occurs when there are problems with the login information. The most common cause of an incorrect login message is a mistyped password. Make sure the that correct password is being used, and then attempt to enter it again. Remember that passwords are case-sensitive, so you cannot interchange uppercase letters and lowercase letters. In the same way, the letter "o" is not interchangeable with the numeral "0" nor is the letter "1" interchangeable with the numeral "1."		
Permission denied	This message occurs when there are login, passivord, or NISI security problems. Most often, an administrator has locked the user's password or the user's account has been terminated.		

Table 10-13 Login Problems at the Command Line (Continued)

Login Problem	Description		
Passworti will not work at lookscreen	A common error is to have the Caps Lock key on, which causes all letters to be uppercase. This does not work if the password contains lowercase letters.		
No shell	This message occurs when the user's shell does not exist, is typed incorrectly, or is wrong in the /etc/passwd file.		
No directory! Logging in with	This message occurs when the user cannot access the home irectory for one of the following reasons: An entry in the /etc/pessad file is incorrect, or the home directory has been removed or is missing, or the home directory exists on a mount point that is currently unavailable.		
Choose a new password followed by the New password: prompt)	This message occurs the first time a user logs in and chooses an initial password to access the account.		
Couldn't fork a process!	This message occurs then the server could not fork a child process during login. The most common cause of this message is that the system has reached its maximum number of processes. You can either kill some unneeded processes (if you are already logged into that system as root) or increase the number of processes your system can handle.		

Login Problems in the CDE

Problems associated with logging into the CDE range from a user being unable to login (and returning to the CDE login screen), to the castom environment not loading properly. In general, the system does not return error messages to the user from the CDE. The following is a list of files and directories that provide troubleshooting information about the CDE:

/usr/dt/bin/Xsession

This file is the configuration script for the login manager. This file should not be edited. The first user-specific file that the **Xaesslon** script calls is the **SHOME**/.dtprofile** file.

SHOME/.drgrofile

By default, the file does not contain much content, except for examples. It contains a few echo statements for session logging purposes, and the DISCURCEPROFILE variable is set. But it also contains information about how it might be edited. The user can edit this file to add user-specific environment variables.

DISOURCEPROFILE=true

This line allows the user's \$HOME/.login file (for csh users) or the \$HOME/.profile (for other shell users) to be sourced as part of the startup process.

Sometimes a .login or .profile file contains problem commands that cause the shell to crash. If the .dtprofile file is set to source a .login or .profile file that has problem commands, desktop startup might fail.

Consequently, no desktop appears. Instead, the system redisplays the Solaris OE CDL login screen. Startup crops from the .log_n or .profile file are usually noted in the SHLME/.dt/startlog file. Use a Failsafe login Session or a command-line login to debug problem commands in the .login or .profile files.

• SIGNE/.dt/sessions

This directory structure contains files and directories that configure the display of the user's custom desktop and determine the applications that start when the user logs in. Look for recent changes to files and for changes to the directory structure. For example, examine the home directory and the home old directory or a current directory and the current, all directory. Compare the changes. The changes could provide information on a new application or on changes in the saved desktop that cause the user's login to fail.

• \$9MP/.dt

Upon removing the entire .dc directory structure, log out, and log back in again for the system to rebuild a default .dc file structure. This action allows the user to get back into the system if the problem with the CDE files cannot be resolved.

Table 10-14 shows the locations of and information found in error logs for the CDE.

Table 10-14 DE Error Log Locations

Location	Error Log		
/var/dt/Xerrors	The Solaris OE CDE login window system errors that occur prior to user login		
\$HXQ/.dt/startlog	The Solaris OE CDE errors that occur during the startup of the Xsession script, while processing he .dtprofile, .login, or .profile file		
\$80ME/.dt/errox)eg.eld \$80ME/.dt/erroxlog.elder	The Solaris OE CDE errors that occur after the Xsession script start up		
\$HOME/.dt/sessionlogs	Directory of s ssion logs for Session Manager and Window Manager errors		



Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guidance. Cach bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab provides more guidance. Although
 each step describes what you should do, you must determine the
 commands (and options) to imput.
- Level 3 This version of the lab is the easiest to accomplish because each step provides exactly what you should input to the system. This level also includes the task solutions for all three levels.



Exercise: Adding User Accounts and Group Entries (Level 1)

In this xeroise, you use the Solaris Management Console, as well as the smuser, sugroup, usermed, userdel, groupadd, and groupdel commands, to create, modify, and delete multiple user accounts and group entries.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed. Refer to Table 10-15 and Table 10-16 as needed.

Table 10-15 Group Specifications

Group Name	GID Number			
class1	101			
class2	102			

Table 10-16 User Specifications

User Name	Password	Shell	UID	Primary Group	Secondary Group
user3	123 pass	Korn	1003	10	class1
user4	123раяя	C	1004	10	class1
user5	123pass	Bourne	1005	10	
lockedl	Select Account is Locked	Bourne	2001	10	
clearedl	Select User must set password at next login	Bourne	2002	10	

Tasks

Complete the following tasks:

- Disable the Salaris OE registration window.
 (Steps 1-5 of Task 1 in the Level 2 lab)
- Working from Table 10-15 and Table 10-16 on page 10-37, create two
 new groups and two new users by using the groups discusser commands.

(Steps 1-2 of Tasks 2 and 3 in the Level 2 lab)

- Launch the Solaris Management Console, and create a user template to add users that do not use automounted home directories.
 - (Step 3 of Task 3 in the Level 2 lab)
- Using the Solaris Management Console, add the new users us emb, locked land element with characteristics from Table 10-16 on page 10-37.

(Steps 4-5 of Task 3 in the Level 2 lab)

- Verify that the shells you specify are set in the veric/password file.
 Determine if the password strings for users with the same password are also the same in the /etc/shadow file. Check the password strings for the users locked 1 and cleared 1. Verify that the users users and as er4 are secondary members of the class 1 group.
 - (Steps 1-4 of Task 4 in the Level 2 lab)
- Determine what happens when you try to log in as the user locked. Verify that you can log in as the user cleared. Record the password requirements indicated.

(Steps 5-6 of Task 4 in the Level 2 lab)

- Establish password aging for the user users. Determine what happens when you attempt to log in as that user. Log in as defended to dunge the password from the command line. Log in as the root user when you are finished.
 - (Steps 1-4 of Task 5 in the Level 2 lab)
- Lise the groupsed command to add a group called class3. Use the
 usermod command to change the UID number, home directory, and
 user name for the user Looked1. Verify that the changes exist in the
 /etc/passwd file.

(Steps 1-2 of Task 5 in the Level 2 lab)

• Use the souser command to change the login shell of user5 to kell. Use the userdel command to delete the user user3. Verify that the home directory has been deleted. Use the anguage command to rename the group class1 to group1. Use the groundel command to remove the group class2. Verify the changes to the /etc/group file. (Steps 3-7 of Task 5 in the Level 2 lab)



Exercise: Adding User Accounts and Group Entries (Level 2)

In this exercise, you use the Solaris Management Console, as well as the small, Section, usermed, userdel, groupadd, ind groupdel commands, to create, modify, and delete multiple user accounts and group entries.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed. Refer to Table 10-15 and Table 10-16 on page 10-37 as nexted?

Task Summary

In this exercise, you accomplish the following:

- Disable the Solaris OE registration window.
- Working from Table 10-15 and Table 10-16 on page 10-37, create two
 new groups and two new users by using the commands groupsda,
 suproup, user=dd, and souser.
- Launch the Solaris Management Conside, and create a user template to add users that do not use automounted home directories.
- Using the Solaris Management Cursole, add the new users users, locked1 and cleared1 with characteristics from Table 10-16 on page 10-37.
- Verify that the shells you specify are set in the /etc/pass will ide.

 Determine if the password strings for users with the same password are also the same in the /etc/shadow file. Check the password strings for the users locked and cleared. Verify that the users user3 and user4 are secondary members of the class1 group.
- Determine what happens when you try to log in as the user log ked1. Verify that you can log in as the user cleared1. Record the password requirements indicated.
- Establish password aging for user5. Determine what happens when
 you attempt to log in as that user. Log in as user5 and attempt to
 change the password from the command line. Log in as the root
 user when you are finished.

- Use the groupadd command to add a group called class3. Use the
 use root command to change the UID number, home directory, and
 user name for the user locked1. Verify that the changes exist in the
 /etc/passwd file.
- Use the smuser comman—to change the login shell of user5 to K4.
 Use the userdel command to delete the user user3. Verify that the user's home directory has been deleted. Use the smgroup command to rename the group class1 to group1. Use the groupdel command to remove the group class2. Verify the changes to the /etc/group file.

Tasks

Complete the following tasks.

Task 1 - Disabling the Solaris OE Registration Window

Complete the following steps:

- Disable the Swaris OE Registration window so that it does not appear whenever a new u er logs in from the CDE.
- Log in as the root user (or use the su command to change to the root user).
- 3. Change to the /etc/default directory.
- 4. In the default directory, create the solvegis file.

#vi solregis

- 5. In the solrogis file, type the keyword DISABLE-1 (note that the character "1" is the number one).
- 6. Save this file, and exit the editor.

Task 2 - Adding Group Entries

Complete the following steps:



Note - Refer to Table 10-15 on page 10-37 for details while adding groups.

- 140te Refer to facte 10-15 of page 10-57 for details writte adding groups
- Add the two groups class1 and class2 with the groupadd and sagroup commands, respectively.

As the root user, open a terminal window.

Task 3 - Adding User Accounts

Complete the following steps:

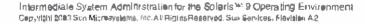


Note – Refer to Table 10-16 on page 10-37 for details while adding users with the various tools.

- 1. Add a user named user3 by using the userade command.
- Add a user named user4 by using the smuser command.
- 3. Launch the Solaris Management Console by typing sace on the command line. After the Solaris Management Console appears, treate a user template to add user accounts that do not use nutrimounted home directories by performing the following:
 - a. Select This Computer, and then select System Configuration. Then select Users, and then select User Templates to open the User Templates tool.
 - From the Menu Bar, select Action. Then select Add User Template.
 - c. The Add User Template window appears, containing blank fields for a template name and description. Enter the name 239user in the User Template Name field, and \$3239 for the Description field.
 - d. Click the Home Directory Tab and uncheck the Automatically Mount Home Directory check box. Enter the name of your system in the Home Directory Server field.
 - e. Click OK to create your template.
- 4. Click User Accounts, and add the user5 account by selecting Action, then selecting Add User, and then selecting From Template on the ment bar.

The Add User From Template window appears. Enter user5 in the User Name field, and select 1005 as the User ID Number. For the password, click User Must Use, and enter 123 pass in both priss word fields. Click OK.

5. From the Solaris Management Console, add additional users locked and cleared by using the 239user template. While adding the cleared user, select the password option User Must Set Password At Next Login. After adding both users, double-click the Locked user and select the tab General. Under the Account Availability section, select the button Account is Locked. Also select the shell as listed in Table 10-16 on page 10-37.



Task 4 – Examining Configuration Files

Complete the following steps:

- Examine the contents of the /etc/passwd file. What are the full path names of the shells used by user 3, user 4, and user 57
- Examine the contents of the /ecc/shadow file. What text is found in the password field for the users looked1 and cleared1?
- You used the same password for user3 through user5. Am the password strings the same in the /eto/shadow file?
- 4. Examine the contents of the /etc/group file. Verify that user3 and user4 are both listed as secondary members of the classil group. Are they?
- 5. Log out of the CDE, and attempt to log in as locked. Are you able to log in?
- 6. Attempt to log in as clearess. What happens? Attempt to use the password chodetg. What are the system requirements for the password?

Use the password about 23. Log in as cleared latter you establish a password to verify that the login works. Log out, and log in as the root user.



Task5 - Establishing Password Aging

Complete the following steps:

Start the Solaris Management Console, and go back into the User Accounts Tool. Select user5 from the list of users. Change the password options information for user5 so that it matches the following information. Click •K when you are frished, and exit the Solaris Management Console.

User Must Keep For: 1 (one day)
Before Change Alert User: 1 (one day)
User Must Change Within: 2 (two days)
Expires If Not Used For: 1 (one day)

2. Log out of your root login session. Attempt to log in as users. What happens? Supply a new password if necessary.

- 3. Complete the login as user5. Open a terminal window, and attempt to change the password you just set. What happens?
- 4. Log out, and log in again as the root user.

Task 6 - Modifying User Accounts and Group Entries

Complete the following steps:

- Use the gro-paid command to create a new group entry called class that uses GID number 103.
- 2. Use the issermed command to change the login name of locked1 to user6, the UID to 3001, and the home directory of locked1 to user6. Verify that the changes you request are exorded in the /etc/passed file and the directory that was moved.
- Use the **meer modify command to change the login shell of user5
 to /bin/kst. Verify that the changes you request are recorded in the
 /etc/possed file.
- 4. Use the userdel command to delete the user account cleared; and the related home directory. Verify that the /export/home/cleared1 directory no longer exists.
- 5. Use the sagroup mornal to change the group name of class1 to group.
- 6. Use the groupdel command to remove the group entry class2.
- 7. Verify that the commands used to modify group entries have correctly modified the /etc/9000 file.

Exercise: Adding User Accounts and Group Entries (Level 3)

In this exercise, you use the Solaris Management Console, as well as the surser, sugroup, usermed, userdel, groupedel, grouped, and groupedel commands, to create, modify, and delete multiple user accounts and group entries.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed. Refer to Table 10-15 and Table 10-16 on page 10-37 as needed.



Note - Some of the commands displayed in this section are quite long and will wrap to the next line. You should consider all of the bold typeface commands that follow a command line prompt to be all one line.

Task Summary

In this exercise, you accomplish the following:

- Disable the Solaris OE registration window.
- Working from Table 10-15 and Table 10-16 on page 10-37, create two
 new groups and two new user accounts using the commands
 groupadd, angroup, useradd, and sauser.
- Launch the Solaris Management Console and create a user template to add users that do not use automounted home directories.
- Using the Solaris Management Consule, add the new user accounts users. Lockedl, and clearedl with characteristics from Table 10-16 on page 10-37.
- Verify that the stiells you specify are set in the /eco/passwo file.
 Determine if the password strings for users with the same password are also the same in the /eco/shadow file. Check the password strings for the users looked and cleared. Verify that the users user? and user4 are secondary members of the classifigroup.
- Determine what happens when you hay to log in as the user lookeds. Verify that you can log in as the user cleaneds. Record the passiverd requirements indicated.

- Establish passivord aging for the user user5. Determine what
 happens when you attempt to log in as that user. Log in as user5
 and attempt to change the password from the command line. Log in
 as root when you are finished.
- Use the groupedd command to add a group called class.3. Use the
 usermed command to change the UID number, home directory, and
 user name for the user locked1. Verify that the changes exist in the
 /etc/pessed file.
- Use the wineer command to change the login shell of user5 to keh.
 Use the userdel command to delete the user3 account. Verify that
 the user's home directory has been deleted. Use the sngroup
 command to rename the group classift to group!. Use the groupdel
 command to remove the group class2. Verify the changes to the
 /etc/group file.

Tasks and Solutions

Complete the following tasks.

Task 1 - Disabling the Solaris OE Regist ration Window

Complete the following steps:

- Disable the Sharis OE Registration window so that it does not appear whenever a new user logs in from the CDE.
- Log in as the root user (or use the su annument to change the root user).
- 3. Change to the /et.c/default directory.
- 4. In the default directory, create the file solvegis.

vi solregis

- In the solvest's file, type the keyword DIGABLE=1 (note that the character "1" is the number one).
- 6. Save this file, and exit the editor.

Task 2 - Adding Group Entries

Complete the following steps:



Note - Refer to Table 10-15 on page 10-37 for details while adding groups.

- As the root user, open a terminal window.
- Add the two groups class1 and class2, with group add and engroup communds, respectively.
- # groupadd -g 101 class1
- # /usr/sadm/bin/segroup add --- -n class2 -g 102

Task 3 - Adding User Accounts

Complete the following steps:



Note - Refer to Table 10-16 on page 10-37 for details while adding users with the various tools.

1. Add a user named users by using the useraid convinand.

useradd -u 1003 -g 10 -G clase1 -d /export/home/user3 -m -e /bin/ksh user3

passwd user3

Yew Passwind: 123pass

Re-enter Password: 123pane

passwel: password successfully changed for user3

2. Add a user named user4 by using the smuser command.

/usr/cametric/senser and -- -n users -u 1004 -g 10 -G class1 -d /export/home/users -s /hin/ceh -z outchers-N

♥ passwd user4

New Password: 123pass

Re-enter new Password: 123 pass

passod: password successfully changed for user4

- 3. Launch the Solaris Management Console by typing amor on the command line. After the Solaris Management Console appears, create a user template to add user accounts that do not use automounted home directories by performing the following:
 - Select This Computer, and then select System Configuration.
 Then select Users, and then select User Templates to open the User Templates tool.

- From the Menu Bar, select Action, and then select Add User Template.
- c. The Add User Template window appears, containing blank fields for a template name and description. Enter the name 239 user in the User Template Name field, and \$A239 for the Description field.
- d. Click the Home Directory Tab and uncheck the Automatically Mount Home Directory check box. Enter the name of your system in the Home Directory Server field.
- e. Click OK to create your template.
- Click User Accounts, and add the user5 account by selecting Action, then selecting Add User, and then selecting From Template on the menu bar.

The Add User From Template window appears. Enter user E in the User Name field and select 1005 as the U1D Number. For password, click the button called User Must Use, and enter 123pass in both password fields. Ack OK.

5. From the Solaris Management Console, add the users locked and observed by using the 230 user template. While adding the eleared luser select the password option User Must Set Password At Next Login. After adding both users, double-click the locked user and select the tab General. Under the Account Availability section, select Account is Locked. Also select the shell as listed in Table 10-16 on page 10-37.

Task 4 - Examining Configuration Files

Complete the following steps:

 Examine the contents of the /etc/pssmofile. What are the full path names of the shells used by user3, user4, and user5?

user3	/oin/kah
user⁄i	/bin/ceh
user5	/bi.n/sh

Examine the contents of the /etc/shadow file. What text is found in the password field for the users looked1 and oleared1?

Locked1

LK

cleared

nene

- You used the same password for user3 through user5. Are the password strings the same in the /etc/shadow file?
- 4. Examine the contents of the /etc/group file. Verify that user3 and user4 are both listed as secondary members of the class1 group. Are they?

The names user3 and user4 should be listed in the last field for the classal group.

- 5. Log out of the GDE, and attempt to log in as 1-acked1. Are you able to log in?
 - No, you get a message that says lowin incorrect, no matter what you use as a vasacord.
- 6. Attempt to log in as cleared. What happens? Attempt to use the password abodefy. What are the system bequirements for the password? You must not press Return when you are asked for an initial password.

You must choose an initial password for this user and then toy in again. The first fix characters must contain at least two alphabetic characters and at least-room numeric or special character.

Use the password abc123. Log in as clear=d1 after you establish a password to verify that the login works. Log out, and log in as the root user.

Task 5 - Establishing Password Aging

Complete the following steps:

 Start the Solaris Management Console, and go back into the User Accounts tool. Select user5 from the list of users. Change the passward options information for user5 so that it matches the following information. Click OK when you are finished, and exit the Solaris Management Console.

User Must Keep For: 1 (one day)
Before Change Alert User: 1 (one day)
User Must Change Withia: 2 (two days)
Expires If Not Used For: 1 (one day)

 Log out of your root login session. Attempt to log in as users. What happens? Supply a new password if necessary.

You numi supply a new password before you can log in-

 Complete the login as user5. Open a terminal window, and attempt to change the password you just set. What happens?

When you log in, a warning indicates that your password expires in two

When you try to change your password, the following error message appears:

passed: Serry: less than 1 days since the last coange. Permission denied

4. Log out, and log in again as the root user.

Task 6 - Modifying User Accounts and Group Entries

Complete the following steps:

 Use the groupedd command to create a new group entry called class3 that uses GID number 103.

groupadd -g 103 clasa3

 Use the usermod command to change the login name of locked1 to user6, the UID to 3001, and the home directory of locked1 to user6. Verify that the changes you request are recorded in the /etc/passwd file and that the directory was moved.

usermail -u 3001 -d /export/home/user6 -m -1 user6 locked1

The /ecc/3009vd file should reflect the new LHD number and user name. The directory under /export/home should be renamed.

Use the smuser modify command to change the login shell of users
to /min/ksh. Verify that the changes you request are recorded in the
/etc/passed file.

/war/sam/bin/smuser workly -- -n wer5 -s /bin/ksh

The /etc/pasawi file should show that the shell is /bin/kah.

 Use the userdel command to delete the user account cleared1 and the related lume directory. Verify that the /expert/neme/cleared1 directory no longer exist.

userdel -r cleared1

The /export/home/cleared directory should no longer enlet.

5. Use the singroup command to change the group name of class1 to group.

/usr/sadm/bin/smgroup modity -- -n classi -N group1

6. Use the groupdel command to remove the group entry class?.

groupdel class2

7. Verify that the commands used to modify group entries have correctly modified the /etc/group file.

The group group1 should exist. The groups class1 and class2 should not exist.

Exercise Summary



Discussion - Take a few minutes to discuss what expediences, issues, or discoveries you had during the lab exercises.

- Experiences
- Interpretations
- Conclusions
- Applications



Managing Initialization Files

The environment maintained by the shell includes variables that are defined by the login program, the system initialization files, and the user initialization files.

When users log in to the system, their login shells look for and execute two different types of initialization files. The first type controls the system-wide environment. The second type controls the user's environment. The six shells available in the Solaris 9 OE provide basic features and a set of variables which the noot user or a regular user can set in the initialization files to customize the shell environment.

The shells support two types of variables:

- Environment variables Variables that provide information about the user's environment to every shell program that is started.
- Local variables Variables that affect only the current shell. Any subshell started would not have knowledge of these variables.

Introducing System-Wide Initialization Files

As the system administrator, you maintain the system-wide initialization files. These files provide an environment for the entire community of users who log in to the system. The Solaris OE provides the system initialization files. They reside in the /eto directory.

The /etc/profile file and the /etc/.login file are the two main system initialization files.

The Bourne, Korn, and BASH login shells look for and execute the system initialization file /ecc/psofile during login.

The C login shell looks for and executes the system initialization file /etc/.109in during the login process.

There are no default global initialization files for the Z or TC shells.



Note — The default files /ctc/profile and /etc/.login theck disk usage quotas, pri t the message of the day from the /etc/motd file, and check for mail. None of the messages are printed to the screen if the hushlogin file exists in the user's home directory.

Introducing User Initialization Files

As the system administrator, you set up the user initialization files that are placed in each user account's home directory when the user is created.

The primary purpose of the user initialization files is to define the characteristics of a user's work environment, such as the command-line prompt, the environment variables, and the windowing environment.

Only the owners of the files or the root user can change or customize the content of these files.

Table 10-17 shows the initialization files necessary for each primary shell available in the Solaris 9 OE.

Table 10-17 Initialization Files for the Primary Shells

Shells	System-Wide Initialization Files	Primary User Initialization Files Read at Login	User Initialization Files Read When a New Shell Is Start	Shell Path Name
Bourne	/etc/profile	SHOME/.profile		/bin/sh
Korn	/etc/profile	SMONG/ profile \$HCME/.kshrc	\$HCME/.kshrc	/bin/ksh
С	/etc/.login	\$HOME/.cshrc SHWE/.login	SHOME/.cshrc	/bit:/cst.

For additional information about the Z. BASH, and TC shells available in the Solaris 9 OE, refer to the online manual pages.



Note - By default, the root user's login shell is the Bourne shell, and the shell entry in the /eto/passwd file appears as /sbin/eta.

When a user logs in to the system, the system invokes the user's login shell program. The shell program looks for its initialization files in a specific order, executes the commands contained in each file, and displays the shell prompt on the user's screen.

Customizing the User's Work Environment

The Solaris OE provides a set of initialization file templates. The /etc/sicel directory contains the initialization file templates. Table 10-18 shows the default initialization file templates and the user initialization files for the Boune, Korn, and C shells.

Table 10-18 Default User Initialization Files

Shell	Initialization File Templates	User Initialization Files
Bourne	/etc/skel/local.profile	SHOME/.profile
Korn	/etc/skel/local.profile	\$HOME/.profile
C	/etc/skel/local.cshrc /etc/skel/local.login	\$HOME/.cshrc \$HOME/.legin



Note - The useradd command copies files from the /etc/skel directory to the \$HOME directory. The smuser command copies files from the /etc/skel directory to the \$HOME directory and renames them to the appropriate file names.

The root user can customize these templates to create a standard set of user initialization files. A standard set of user huitialization files provides a common work environment for each user. When the root user creates new user accounts, some or all of these initialization files are automatically copied to each new user's home directory.

Users can then edit their initialization files to further customize their environments for each shell.

Table 10-19 shows some of the wriables available for customizing a user's shell environment.

Table 10-19 Login Variables

Variabl e Name	Set By	Description				
LOGNAME	Login	Defores the user's login name.				
HCME Login		Sets the path to the user's home directory. It is the default argument for the cd command.				
SHELL	Legin	Sets the path to the default shell				
PATH	Login	Sots the default path that the shell searches to find commands				
MAIL	Largin	Sets the path to the user's mailbox.				
TERM	Login	Defines the terminal.				
LPDEST	Not ser by default	Sets the user's default printer.				
PWD	Shell	Defines the current working directory.				
PSl	Shell	Defines the shell prompt for the Bourne or Korn shell.				
prompt Shell		Defines the shell pro pt for the C shell.				



Note – For complete information on all variables used by the default shells, see the following man pages: sh(1), sh(1), sh(1), sh(1), sh(1), sh(1), sh(1).

A itser can change the values of the predefined variableand specify additional variables.

Table 10-20 shows how to set environment variables in the user initialization files of the Bourne, Korn, and C shells.

Table 10-20 Setting Environment Variables

Shell	User's Initialization File			
Bourne or Korn	VARIABLE=value ; export VARIABLE For example: PS1=*SFFENDE*; export PS1			
С	setenv variable value For example: setenv LPDEST laserprinter			



Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guidance. Each bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab Provides more guidance. Although
 each step describes what you should do, you must determine the
 commands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because each step provides exactly what you should input to the system. This level also includes the task solutions for all three levels.



Exercise: Modifying Initialization Files (Level 1)

In this exercise, complete the following tasks:

- Modify initialization file templates in the /etc/ske1 directory
- Create user accounts that use the initialization files

Preparation

This exercise requires the skills practiced in the previous exercise. The user accounts that you create in this exercise are required in later sections of the course. Refer to the lecture notes as necessary to perform the tasks listed.

Tasks

Complete the following tasks:

Modify the template for Bourne; shell users. Set the EDITOR to vi.
LEDEST to printex1, EXINT to set showed autoindent and
number, and ENV to source the .kshrs file.

(Steps 1-3 in the Level 2 lab)

• Use the Solaris Management Console to create a new user account collect user? that uses the Korn shell. Log in tasthe new user, and verify that all the variables you set in local .profile are set correctly in the user's environment.

(Steps 4-6 in the Level 2 lab)

- Create a kehr c file for the new user account that includes two
 aliases and sets the primary prompt to echo the current working
 directory. Log out, and log in again as the same user to verify that
 the kehr c file works. Log out, and log in again as the root user.
 (Steps 7-9 in the Level 2 lab)
- Use the useradd command to create a new user account called user10 that uses the Korn shell. Log in as this user, and record the list of initialization files in the home directory. Copy the appropriate file to the "profile file. Test the login to verify that the list of variables is set the same as those of the first user you created. Log out, and log in as the root user when you are finished.

(Steps 9-13 in the Level 2 lab)

Exercise: Modifying Initialization Files (Level 2)

In this exercise, complete the following tasks:

- Modify initialization file templates in the /exc/skel directory
- Create user accounts that use the initialization files

Preparation

This exercise requires the skills practiced in the previous exercise. The user accounts that you create in this exercise are required in later sections of the course. Refer to the lecture notes as necessary to perform the tasks listed.

Task Summary

In this exercise, you accomplish the following:

- Modify the template f r Bourne shell users. Set the EDITOR to vi, t.PDEST to printer, EXENIT to set showned autoindent and number, and ENV to source the . Aspec file.
- Use the Solaris Management Consoleto create a new user account called users that uses the Korn shell. Log in as the new user, and verify that all the variables you set in local .profile are set correctly in the user's environment.
- Create a katero file for the new user account that includes two
 aliases and sets the primary prompt to echo the current working
 directory. Log out, and log in again as the same user to verify that
 the ketter file works. Log out, and log in again as the root user.
- Use the useracid command to create a new user account called user 10 that uses the Korn shell. Log in as this user, and record the list of initialization files in the home directory. Copy the appropriate file to the "profile file. Test the login to verify that the list of variables is set the same as those of the first user you created. Log out, and log in as the root user when you are furtished.

Tasks

Complete the following steps:

- 1. Log in as the most user, and open a terminal window.
- 2. Change to the /etc/skel directory.
- Use the vi editor to edit the local .mrofile file, and make the following changes:
 - Edit the line that declares the PATH variable so that it reads as follows. Enter this text as one line (no spaces).

PATH=/usr/sbin:/ebin:/usr/sadm/bin:/usr/dt/bin:/usr/openwin/bin:/usr/bin:/usr/openwin/bin/bin/usr/openwin/

 Add the following lines below the FHH wriable you just edited:

EDITOREVI

LPDEST-printer1

EXTYT='set chommods autoindent number' ENV=\$HOME/.kshrc

c. Change the line that mods:

export PATH

so that it reads:

export PATH EDITOR LPDEST CXINIT ENV

4. Use the Solaris Management Console to create a new user account with the following characteristics. Exit the Solaris Management Console when you are finished.

User Name: user9
User ID: 1009
Primary Group: staff
Login Shell: Korn
Password: 123 pass

- 5. Log out, and log in again as user. Open a terminal window.
- Verify that the PATH, LPDEST, EDITOR, EXEMIT, and ERW variables are set according to the changes you made in the /etc/skel/local.profile file.

Do they makeli?

Create a file called "kaher in user9's home directory.
 Insert the following lines. A space follows the SPDS in the last line.

set -o noclobber set -o ignoresof alias hehistory alias coclear PS1="SPMD\$"

> Log out, and then log in again as users. Open a terminal window, andverify that your new variables work.

Do they work?

 Log out, and log in again as the root user. Use the useradd command to create a new user account called user10 with the following characteristics:

User Name: user10
User ID: 1010
Primary Group: 10
Login Shell: Korn
Home Directory: /export/remo/user10
Comment: SA-239 Student
Password: congetin

- 10. Log out, and log in again as user10. Open a terminal window. What shell initialization files exist in your home directory?
 - Which of these are the stame as /etc/skel/local.profile?
- 11. Copy the local profile file to the . profilefile.
- 12. Log out, and log in again as user 10. Verify that the variables set for the user 9 login are also set for this login.

Do they match?

13. Log out, and log in again as the root user.

Exercise: Modifying Initialization Files (Level 3)

In this exercise, complete the following tasks:

- Modify initialization file templates in the /etc/skel directory
- Create user accounts that use the initialization files

Preparation

This exercise regulars the skills practiced in the previous exercise. The user accounts that you create in this exercise are required in later sections of the course. Refer to the tecture notes as necessary to perform the tasks listed

Task Summary

In this exercise, you accomplish the following:

- Edit the /etc/skel/local.profile fileso that it sets the PATH variable to a specific list of directories. Set the EDITOR, LIPEST, EMINIT, and ENV variables to appropriate values.
- Use the Solaris Management Console to create a new user account cailed user? that uses the Korn shell. Log in as the new user, and verify that all the variables you set in local profile are set correctly in the user's environment.
- A kehro file for the new user account that includes two almost and sets the primary prompt to echo the current working directory. Log out, and log in again as the same user to verify that the kehro file works. Log out, and log in again as the root user.
- Use the user add currenand to create a new user account called user10 that uses the Korn shell. Log in as this user, and record the list of initialization files in the home directory. Copy the appropriate file to the .pxofile file. lest the login to verify that the list of variables is set the same as those of the first user you created. Log out, and log in as the root user when you are finished.

Tasks and Solutions

Complete the following steps:

- 1. Log in as the root user and open a terminal window.
- 2. Change to the /etc/akel directory.

od /etc/skel

Use the vi editor to colt the local.profile file, and make the following changes:

vi local.profile

 a. Edit the line that declares the PATH variable so that it reads as follows. Enter this text as one line (no spaces).

PATH=/usr/abin:/sbin:/usr/sadm/bin:/usr/dt/bin:/usr/openvio/bin:/usr/bin:/usr/ucb:.

Add the following lines below the PAPE variable you just edited:

COLVILLE VI

LFUEST-printer1

CXDVT='set showed autoindent number ENV=\$HORE/.kehrc

c. Change the line that reads:

export PATH

so that it reads:

export PATH EDITOR LPDEST EXINIT ENV

 Use the Solaris Management Console to create a new user with the following character istics. Exit the Solaris Management Console when you are finished.

User Name: user9
User ID: 1009
Primary Croup: staff
togin Shell: Korn
Password: 123pass

5. Log out, and log in again as user9. Open a terminal window.

- 6. Verify that the MAN, EFERSE, EDITOR, EXEMPT, and ENV variables ansect according to the changes you made in the /etc/skel/local.profile file.
- \$ echo \$PATH
- \$ echo \$LPIEST
- \$ acho SEDTTUR
- \$ echo \$@CINTE
- \$ ocho \$ENV

Do they match?

These variables should match the settings made in the local.profile file.

- 7. Create a file called . kshrc in users's home directory.
- \$ cd
- 5 vi. .kshrc

Insert the following lines. A space follows the \$PADS in the last line.

set -o arrighter set -o ignoresof elias hehistory alias c=clear PS1='\$PWD\$'

5. Log out, and then log in again as users. Open a terminal window, and verify that your new variables work.

\$ cd /tmp

\$ cd

\$ c

\$ h

Do they work?

These variables should function according to the values set in . ksrccc. The proupt should reflect your current directory, and the aliases should clear the screen and present a history list.

 Log out, and log in again as the root user. Use the useradd command to greate a new user account called user10 with the following characteristics:

User Name: user10
User ID: 1010
Primary Group: 10
Login Shell: Korn

Home Directory: /export/home/user10

Comment: SA-239 Student

Password: cangetin

* userafit -n 1010 -g 10 -ā /export/home/user10 -m -s /bin/hah -c *8A-239 Student- user10

64 blacks

passwd user10

New password: carrotin

Re-enter new password: cangetia

10. Log out, and log in again as user 10. Open a terminal window. What shell initial: Inlion files exist in your home directory?

S 18 -1a

.profile, local.profile, focal.login, local.cshire

Which of these are the same as the /etc/skel/local.profile file? The local.profile file.

II. Copy the rocal .profile file to the .profile file.

S cp local.profile .profile

- 12 Log out, and log in again as user 10. Verify that the variables set for the user 3 login are also set for this login.
- S echo SPATH
- \$ echo \$LFIEST
- \$ echo \$EDITOR
- \$ echo \$EXIRUT
- \$ echo \$ENV

Do they match?

These variables should match the settings made in the iscal profile

13. Log out, and log in again as the root, user.

Exercise Summary



Discussion – Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exermises.

- Experiences
- Interpretations
- Conclusions
- Applications



Performing System Security

Objectives

Upon completion of th'ismodule, you should be able to:

- Monitor system access
- Switch users on a system
- Control system access
- Restrict access to data in files

The following course map shows how this module fits into the current instructional goal.

Performing User and Security Administration

Performing User Administration

Performing System Security

Figure 11-1 Course Map

Monitoring System Access

All systems a ould be monitored routinely for unauthorized user notess. You can determine who is or who has been logged into the system by executing commands and examining log files.

Displaying Users on the Local System

The who command displays a list of users currently logged in to the local system. It displays each user's login name, the login device (TTY port), the login date and time. The command reads the binary file /var/acm/ution to obtain this information and information about where the users logged in from.

If a user is logged in remotely, the who command displays the remote hust name, or Internet Protocol (IP) address in the last column of the output.

iİ	OUM
115	3 200
r	cat
<u> </u>	oot.
I	oct
큐	

pts/2 pts/5	2500	13:53 09:22	(sys43) (129.147.4.13)
pts/3 console		14:27 11:05	(ਬੱye €1) (±3)

The second field displayed by the who command defines the user's login device, which is one of the following:

- console The device used to display system boot and error messages
- pts The pseudo device that represents a login or window session without a physical device
- berm The device physically connected to a serial port, such as a terminal or a modern



Note — The who command has many options, one of which is the —m option. The who —n command outputs information about only the current terminal window.

Displaying Users on Remote Systems

The rusers command produces output similar to that of the who command, but it displays a list of the users logged in on local and remote hosts. The list displays the user's name and the host's name in the order in which the responses are received from the hosts.

A remote host responds only to the rusers command if its rpc . rusered daemon is enabled. The rpc, rusers@daemon is the network server daemon that returns the list of users on the remote hosts.



Note - The full path to this network server daemon is /usr/lib/netave/rusers/fpc, rusersd.

The following is the command format for the rusers command:

rusers -options hostname

The rusers —I command displays a long list of the login names of users who are logged in on local and remote systems. The output displays the name of the system into addich a user is logged, the login device (ITY port), the login date and time, the idle time, and the login host name. If the user is not idle, no time is displayed in the idle time field. The term idle means that the user is not actively doing anything at the time on the terminal, which would denote the user is probably at screen lock or away from the terminal.

The following is an example of the rusers command:

rusers -1

Senci_nç	broadcast for rusered proto	col	version 3.		
IOCT	instructor:console	Feb	5 11:05	50:15	(:0)
rect	instructor:pts/5	Feb	6 09:22	27:38	(129.147.4.13)
root	instructor:pts/6	1 eo	4 13:36	5:08	(129.147.48.219)
root	insuructor:pta/7	Feb	4 13:36	25:50	(129.147.48.219)
root	instructor:pts/2	Peb	6 09:23	27:10	(129.147.4.13)
Yout	imstructer:pts/10	Fab	7 07:35	45	:lightbandit;
root	instructor:pte/12	7eb	7 09:38	44	(lightbendit)
root	irstructor:pts/11	reb	7 14:16		(129.147.4.20)
user2	57544:pts/2	F-1	7 13:53	45	(instructor)
Icol	sys11ext:consc!e	Геb	6 13:17	23:52	
uscr2	≨ys41:pts/1	Feb	7 13:45	44	(instructor)
100C	sys41:pt\$/3	Feb	7 14:32		(instructor)
Sending	broadcast for rusered Proce	col	versi en 2.		

Displaying User Information

To display detailed information about user activity that is either local or remote, use the finger command.

The finger command displays:

- The user's login name
- The home directory path
- The login time
- The login device name
- The data contained in the comment field of the /eco/passwd file (usually the user's full name)
- The logist shell
- The name of the host, if the user is logged in remotely, and any idle time

The following is the command format for the finger command:

```
finger [-bfhilmpgsw] [username...]
finger [-1] [ username@hostname! [ @hostname ]]
```

The -moption matches arguments only on username (not the first or last name that might appear in the comment field of /etc/passwe).

To di play information for usera, perform the command:

finger -m msera

```
Legin name: usera In real life; Alpha User located in Office #4
Directory; Thoma/usera Shall; /bin/sh
On since Dec 17 10:32:53 on console from :0
1 minute 47 seconds Idla Time
We unread rail
No Plan.
```

If users create the standard ASCII files .planor .project in their home directories, the content of those files is shown as part of the output of the finger command.

These files are traditionally used to outline a user's current plans or projects and must be created with file access permissions set to 644 (yy/z=-y-).



Note - You get a response from the finger command only if the in. fingers deemon is enabled.

Displaying a Record of Login Activity

Use the last command to display a record of all logins and logouts with the most recent activity at the top of the output. The last command reads the binary file /var/adm/wmmx, which records all logins, logouts, and reboots.

Each entry includes the user name, the login device, the host that the user is logged in from, the date and time that the user logged in, the time of logout, and the total login time in hours and minutes, including entries for system reboot times.

The output of the Last command can be extremely long. Therefore, you might want to use it with the -n number of lines to display.

The following is an example of the last command:

last user9 console :0 Mon Dec 17 10:3\$ still legged in reet pts/4 129.147.4.12 Mon Dec 17 10:33 still legged in usera console :0 Mon Dec 17 10:32 - 10:38 (00:05) reboot system beat Fri Dec 14 09:58 (output irrancated)

You can use the last command also to display information about an individual user if you supply the user's login name as an argument.

last user9

user 9	ccasel≡	:0	Hor.	Dec	17	10:38		still	Logged	in
≌ετ9	console	: 0	$\underline{F}\underline{x}\underline{i}$	Dec	14	10:13	_	10:25	(00:07	7}
(eutput :	trustated)									

To view the last five system reboot times only, perform the conuncted:

# last	-m 5 reboot	
rebeat	system boot	Wed Feb 20 13:20
reboot	system boot	Wed Feb 20 13:18
rebook	System boot	Fri Feb 1 13:46
r.epcet	system boot	Thu Jan 17 09:02
rebook	system boot	Thu Jan 17 08:55

Performing System Security
Copyright 2003 Sun Microsystems, India All Hights Recoved, Sun Services, Revision A.2

Recording Failed Login Attempts

When a user logain to a system either locally or remotely, the logain program consults the /etc/passwi and the /etc/shadow files to authenticate the user. It verifies the user name and password entered.

If the user provides a login name that is in the /etc/passwd file and the correct password for that login name, the login program grants access to the system.

If the login name is not in the /etc/passwd file or the password is not correct for the login name, the login; program devices access to the system.

You can log failed command-line login attempts in the /var/ada-/loginleg file. This is a useful tool if you want to determine if attempts are being made to break into a system.

By default, the loginlog file does not exist. To enable logging, you should create this file with read and write permissions for the courser only, and it should belong to the sys group.

- # touch /var/adm/loginlog
- # chown root: sys /var/adm/loginlog
- # chand 600 /var/adm/loginlog

All failed command-line login activity is written to this file automatically after five consecutive failed attempts.

The 100 inlog file contains one entry for each of the failed attempts. Each entry contains the user's login name, login device (TTY port), and time of the failed attempt.

If there are fewer than five consecutive failed attempts, no activity is logged to this file.

Switching Users on a System

As the system administrator, you should log in to a system as a regular user, and then switch to the root account only to perform administrative tasks.

You should avoid logging in directly as the root user. This precaution helps protect the system from unauthorized access, because if reduces the likelihood that the system will be left unattended with the root user logged in. Also, critical mustakes are less likely to occur if you perform routine work as a regular system user.

Introducing the su Command

Use the siz command to switch to the superuser or another user without logging out and back in as that user.

The following is the command format for the su command:

sv - usemano

If no user name is given, then the su command attempts to switch to the root user.

To use the su command, supply the appropriate password unless you are already the root user. The root user can run the su command without passwords.

If the password is correct, the su command creates a new shell process, as specified in the shell field of that user account's /eve/passwc file entry.

The sw - (dash) option specifies a complete login by reading all of the user's shell initialization files. The - (dash) option changes your work environment to what would be expected if you had logged in directly as that specified user. It also changes the users home directory.

When you run the su command, the effective user ID (EUID) and the effective group ID (ECID) are changed to the new user to whom you have switched.

Access to files and directories is determined by the value of the EUID and EGID for the effective user, rather than by the UID and CID numbers of the original user who logged in to the system.

Using the who and Command

The whearii command displays the name of the account, whose authorization you have switched to.



Note - The whoami command resides in the /usr/ucb directory.

For example, user1 is logged into the system under that login name. This user then runs the su command to become the root user and enters the root password. The wasani command displays the user's actual authorization for accessing directories and files, for example:

9 whoami userl

\$ pwd

/export/home/userl

S au

password: EnterPeseword

whoard

rcet

DWG

/export/home/user1

Using the who am i Command

To determine the legin name of the original user, use the who command with the an i option.

To use the who an i command, at the shell prompt, type the su command and the login name of the user account to which you want to switch, and press Return. Type the password for the user account, and press Return.

For examile, while logged in as uses1, use the su command to switch to wer2:

\$ su user2

: brewaasq EnterPaceword

5 who am i

use r1

pts/2

Dec 17 12:18

(129,147.4.12)

An alternative to the who an it command is the who im command.

Switching to Another Regular User

To switch to another user and have that user's environment, use the su-command as follows:

1. At the shell prompt, display your login name and path.

\$ who am i

user1 pts/4

Feb \$ 08:38

\$ pwd

/expert/home/userl

Enter the gu command with the dash (-) option and the login name
of the user to which you want to switch. Then, enter the password
for the user.

\$ su - user2

Passwerd: EnterPassword

To determine the login name of the actual user, perform the whoamiconumand, and press Return.

\$ who and

user2

4. To determine the current working directory, perform the pwe command. The location is the effective user's home directory.

\$ pwd

/export/home/user2

5. To display the login name of the original user, perform the who am i command.

\$ who as i

user1

pta/4

Feb 8 08:38

To return to the original user status and home directory, perform the exit command.

\$ exit

\$ pwd

/export/heme/userl

Becoming the root User

In the default system configuration, direct root logins are restricted to the console. This means that you cannot remotely log in to a system as zoot. To remotely log in to a host as the root user, you must log in as a regular user and then run the su command to become the root user.

To become the zoot user, use the su command as follows:

- 1. Log in from the logue window as a regular user, such as user?.
- At the shell prompt in a terminal window, perform the su command.
 Enter the zoot password.

\$ mu - Password: EnterPassword

3. To display the original logur, perform the the are 1 command.

4 who am i

user1

pts/4

Feb 8 88:48

4. To determine the login name of the user to which you have switched, perform the woomi command.

whoami

rent

 To determine the current working directory, perform the pad command.

∌wd ⊭

To exit the root session and return to the original user, perform the exit command.

eveit

\$ pwd

/expert/home/user1

\$

Monitoring su Attempts

For security reasons, you must monitor who has been using the aucommand, especially those users who are trying to gain root access on the system. You can initiate the monitoring by setting two variables in the /eto/default/su file.



Note.—There are many variables in the /etc/default/suffic. This course presents only a small subset of the variables.

Contents of the /etc/default/su File

To display the contents of the /etc/default/su file, perform the command:

cai. /etc/Cafault/gu #ident "C(m)su.dfl 1. 93/08/14 SMI" /* SVx4.0 1.2 */

i SULUG determines the location of the file used to log all su attempts SULUG=/ver/adm/sulcg

COMMONE determines whether attempts to su to root should be logged # to the named device #00NSOLE=/dev/console (output edited for brevity)

5YSLOG=YPS

In the preceding example, unsuccessful attempts to use the succommand to access the root account are logged to the /var/adm/reessages file. The following is an example entry from that file:

Dec 17 12:35:47 sys41 su: IID 810491 auth.crit] 'www.room' failed for users on /dev/pts/2

The console Variable in the /etc/effault/su File

By default, the system ignores the CONSOLE variable in the /etc/default/su file because of the preceding comment (#) symbol. All attempts to use the au command are logged to the console, regardless of success or failure. Here is an example of output to the console:

Feb 2 09:50:09 host1 su: 'su root' failed for user1 on /dev/pts/4 Feb 2 09:50:33 host1 su: 'su user3' succeeded for user1 on /dev/pts/4

When the comment symbol is removed, the value of the ONSCLE variable is defined for the /dev/cmsale file. Subsequently, an additional line of output for each successful attempt to use the su command to socess the most account is logged to the console. Here is an example of logged su command activity:

Feb 2 11:20:07/ host1 su: 'su root' succeeded for user1 on /dev/pts/4 Su 02/02 11:20 : pts/4 user1-root

The sulog Variable in the / default/su File

The SIMOG variable in the /etc/default/su file specifies the name of the file in which all a tempts to use the su command to switch to another user are logged. If the variable is undefined, the su command logging is turned off.

The /var/adm/sulog file is a record of all attempts by users on the system to execute the su command. Each time the su command is executed, an entry is added to the sulog file.

The entries in this file include the date and time the command was issued, whether it was successful (shown by the plus (+) symbol for success or the hyphen (-) symbol for failure), the device from which the command was issued, and, finally, the logic and the effective identity.

The following is an example of entries from the /var/adm/sullog file:

I more /var/adm/sulog

SU 10/20 14:50 + consele rost-sys SU 10/20 16:55 + pts/2 user3-rost SU 11/05 11:21 - pts/3 user1-root

Controlling System Access

The more access that is available over the network, the more beneficial it is for remote system users. However, unrestricted access and sharing of data and resources can create security problems.

A local host's remote security measures are generally based on an ability to validate, limit, or block operations from remote system users.

The /etc/default/login File



Note - There are many variables in the /etc/default/login file. This course, presents only a small subset of the variables.

The /etc/&ciault/login file establishes default parameters for users when they log into the system. The /ent/default/login file gives you the ability to protect the noon account on a system. You can restrict root access to a specific device or to a console, or disallow noot access altogether.

To display the contents of the /ed/fefast-t/login file, perform the command:

```
# cat /etc/default/login
(output edited for brevity)

# If CONSCLE is set, root can only legin on that device.

# Comment this line out to allow remote login by root.

#
CONSOLE=/dev/consele

# PASSREO determines if login requires a password.
```

PASSE TER

The CONSOLEVariable in the /etc/default/login File

You can set the CCNSCLE variable in the /etc/default/login file to specify one of three possible conditions that restrict access to the root account:

 If the variable is defined as CONSOLD=/dev/console, the root user can log in only at the system console. Any attempt to log in as root from any other device generates the error message:

rlogin hostl

Not on system censele Connection closed.

- If the variable is not defined, such as \$CONSOTE / dev/censole, the root user can log in to the system from any device across the network, through a modern, or using an attached terminal.
- If the variable does not have a value assigned to it (for example CONSULE:) then the root user cannot log in from anywhere, not even the consule. The only way to become the root user on the system is to log in as a regular user and then become root, by using the su command.



Note – You can confine root logins to a particular port with the COUNCLE variable. For example, CONSOLE=/dev/term/a permits the root user to log in to the system only from a terminal that is connected to Serial Port A.

The PASSED Variable in the Vetc/default/login File

When the PASSREQ variable in the /etc/default/legin file is set to the default value of VES, then all users who had not been assigned passwords when their accounts were created are required to enter a new password as they log in for the first time. If this variable is set to NO, then null passwords are permitted. This variable does not apply to the root user.

File Transfer Protocol (FTP) Access

The Solaris QE provides an American Standard Code for Information Interchange (ASCII) file named /etc/ftpa/ftpusers. The /etc/ftput/ftpusers file lists the names of users who are prohibited from connecting to the system through the FIP protocol.

Each line entry in this file contains a login name for a restricted user, for example:

username

The FTP server daemon in.ftpd reads the /etc/ftpd/ftpusers file when an FIII session is invoked. If the login name of the user natches one of the listed entries, it rejects the login session and seruls the Login failed enter message.

By default, the /etc/ftpd/fapusers file lists these system account entries:

cent nonesin hin **ร**งร adm lp uucp пиисо Ganne G disten. racbody noaccess nobody4

As with any login name that you can add, these entries must match the user account names located in the /etc/passwd file.

The root entry is included in the ftgusers file as a security measure. The default security policy is to disallow remote logins for the root user. The policy is also followed for the default value set as the CONSOLE entry in the /etc/default/legic file.

The /etc/hosts.equiv and \$HOME/.rhosts Files

Typically, when a remote user requests login access to a local host, the first file read by the local host is its /etc/passad file. An entry for that par cular user in this file enables that user to log in to the local host from a remote system. If a password is associated with that account, then the remote user is required to supply this password at log in to gain system access.

If there is no entry in the local host's /etc/passwd file for the remote user, access is dinnied.

The /att/hosts.equiv and SHOME/. Thosts files bypass this standard password-based authentication to determine if a remoteuser is allowed to access the local host, with the identity of a local user.

These files provide a remote authentication procedure to make that determination.

This procedure first checks the /etc/hosts.equiv file and then checks the SHOME/ , who at file in the home directory of the local user who is requesting access. The information contained in these two files (If they exist) determines if remote access is granted or derived.

The information in the /et.c/mosts.equiv file applies to the entire system, while individual users can maintain their own \$HOME/ .rhosts files in their home directories.

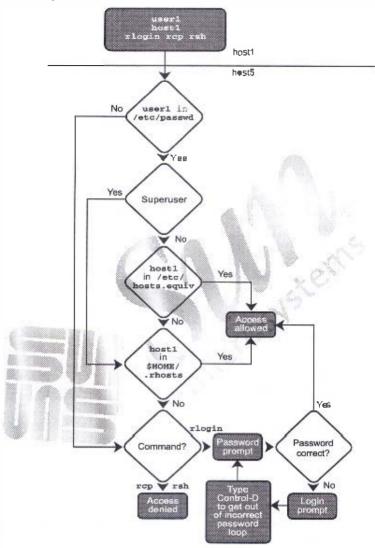


Figure 11-2 shows the flow of remote access authentication.

Figure 11-2 Remote Access Authentication

Entries in the/etc/hosts. equivand \$HONE/.rhosts Files

While the /etc/hosts.equiv and \$HOME/.rhosts files have the same format, the same entries in each file have different effects.

Both files are formatted as a list of one-line entries, which can contain the following types of enhies:

hostname hostname username

The host names in the /etc/hosts.cquiv and \$400B/ rhosts lifles must be the official name of the host, not one of its alias names.



Note - When logging in to a number of different systems, you can run the uname -n command to determine on which system you are currently logged in.

The /etc/hosts.equiv File Rules

For regular users, the /etc/hoses .= ou v file identifies remote hosts and remote users who are considered to be trusted.



Note - The /etc/hosts.equiv file is not checked at all if the remote user requesting local access is the root user.

If the local host's /etc/hosta. equiville contains the host name of a remote host then all regular users of that remote host are trusted and do not need to supply a password to log in to the local host. This is provided so that each remote user is known to the local host by having an entry in the local /ctc/passwd file; otherwise, access is denied.

This functionality is particularly useful for sites where regular users commonly have accounts on many different systems, eliminating the security risk of sending ASCII passwords over the network.

The /ete/nes is, emiv file does not exist by default. It must be created if trusted remote user access is required on the local host.

The SHOME/.rhosts File Rules

While the /etc /hosts .equiv file applies system-wide access for non-root users, the .rhosts file applies to a specific user.

All users, including the root user, can create and maintain their own trhosts files in their home directories.

For example, if you run an rlogin process from a remote host to gain root access to a local host, the / .rhosts file is checked in the root home directory on the local host.

If the remote host name is listed in this file, it is a trusted host, and, in this case, root access is granted on the local bast. The CONSOLE variable in the /eto/default/login file must be commented out for remote root logins.

The SHOME/, thoses file does not exist by default. You must create it in the user's home directory.



Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guidance. Each butleted paragraph provides a task description, but you must determine your own way of accomplishing each lask.
- Level 2 This version of the lab provides more guidance. Although
 each step describes what you should do, you must determine the
 commands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because
 which step provides exactly what you should input to the system. This
 level also includes the task solutions for all three levels.



Exercise: User Access (Level 1)

In this exercise, you complete the following tasks:

- Log failed login attempts
- Use the commands finger, last, misers, su, and who and
- Examine the sulos file
- Change the /et.c/default/legin file to allow reot logins from any terminal
- Change the /ecc/fcpd/fcpusers file to allow FTP access as the root user
- Create a / .rhosts file to allow root access from another system

Preparation

This lab requires two systems that system lists the other its its /etc/inet/hosts file. The lab also requires two specific users, user9 and user3, on both systems. Both users should use the password 123 pass. Refer to the lecture nodes as necessary to perform the steps listed.

Tasks

Complete the following tasks:

Freate alog file to record failed login attempts. Use the commandline login to make five failed login attempts. List the contents of the log file. Use commands to display information for user? on both your system and your partner's system.

(Steps 1-7 in the Level 2 lab)

 Identify when the first root login session on your system occurred and how long the session lasted. Identify when your system last booted. List the users logged in on all systems on your network and on just your partner's system.

(Steps 8-11 in the Level 2 lab)

Change your user identity from the most user to users, both with
and without the - (dash) option. Record the differences, List
effective and real user identity during your su sessions. Locate the
su log and identify which user initiated your su attempts.

(Steps 12-18 in the Level 2 lab)

 As the root user, attempt to log into your partner's system. Record error messages. Change the console variable on your partner's system to allow root logins from any terminal. Attempt to access your partner's system again.

(Steps 19-2) in the Level 2 lab)

 As the cost user, attempt to use the fcp command to access your partner's system. Change the ftp permissions file to allow root access to your partner's system.

(Step 22 in the Level 2 lab)

 As the root user, attempt to use the riogin command to access your partner's system. Ask your partner to create a / riocets file that lists your system name. Attempt to use the riogin command to access your partner's system again.

(Step 23 in the Level 2 Iab)



Exercise: User Access (Level 2)

In this exercise, wu complete the following tasks:

- Log failed login attempts
- Use the commands finger, last, rusers, su, and whom!
- Examine the sulog file
- Change the /etc/default/legin file to allow rook logins from any terminal
- Change the /etc/ftpd/ftpvsers file to allow FTP access as the root user
- Create a /. rhosts file to allow root access from another system.

Preparation

This lab requires two systems. Each system lists the other in its /eto/inet/nosts files. It also requires two specific users, users and users, on both systems. Both users should use the password 120pags. Refer to the lecture notes as necessary to perform the steps listed.

Task Summary

In this exercise, you accomplish the following:

- Create the file /var/adit/loginlog. Use the command-line login to make five falled login attempts. List the contents of the /ver/adit/loginlog file. Use the finger command to display information for user9 on both your system and your partner's system.
- Use the last command to identify when the first root login session
 on your system occurred and how long the session lasted. Use the
 last command to learn when your system last booted, Use the
 rusers command to list the users logged in on all systems on your
 network and on just your paymer's system.

- Use the su command to change your user identity from the root user to user9, both with and without the (dash) option. Record the differences. Use the whears and who am i commands to list your effective andreal user identity during your su sessions. Locate the sulog declared in the /stc/default/su file, and identify which user initiated your su attempts.
- As the root user, attempt a session to your partner's system by
 using the teleast command. Reford error messages. Change the
 Current variable on your partner's system to allow root logins
 from any terminal. Attempt the telest session again.
- As the root user, attempt to use the ftpcommand to access your partner's system. Change the /etc/ftpd/ttpusers file to allow root access to your partner's system.
- As the root user, attempt to use the r login command to access your partner's system. Ask your partner to create a / .rhosts file that lists your system name. Attempt to use the rlogin command to access your partner's system again.

Tasks

Complete the following steps:

- Log in as the root user, and/open a terminal window. Change the directory to /var/adm.
- Use the touch command to create a file called loginlog, (kinsure
 permissions are set to read and write for the root user only.) If
 necessary, set the group ownership to sys.
- 3. Log out. From the CDE Options mean, select the Command Line Login option. When the CDE login screen clears, press Return to obtain the command-line login prompt.
- Enter root after the login prompt, but supply an incorrect password.
 Do this five times. After the fifth attempt, the CDE login screen appears again. Log to as root, and open a terminal window.
- 5. Examine the /var/adm/loginiog file What does it contain?
- 6. Use the finger command to display information for the user called user9. What is the difference in the output between the finger -m command and the finger command with no option?

- 7. Use the finger command to display information for the same user on your pertner's system. (You will need to reference your partner's system on the command line.) Try this with and without the -m option. Does the -m option change the output that the finger ommand displays?
- 8. Use the last command to display login and system reboot activity. When did the first root login occur, and how long did that session last?
- 9. Use the last command to display only system boot activity. When did the system last reboot?
- Use the rusers command to list information about the users on all systems on your network segment.
- 11. Use the rusers command to list information for users on your partner's system. When, and on what terminal, did the first user listed log in?
- 12. Switch your user identity to that of ::ser-9. Do not use the (dash) option.
- 13. Display some of the variables that define your environment.
- Exil the sussession and try to switch your user Identity again, this time using the - (dust)-option.

Are the values reported now correct for the user root or for user??

- 15. Use the whoemi and who ear i commands to list your effective and real user identity.
 - What do these commands report?
- 16. Use the sa command to change your user identity from user9 to user3, and use the whomi and who am i ommands again.

What do these commands report?

Exit both su sessions when you are finished.

- 17. Change the directory to /etc/default. Smovine the /etc/default/sq file, and record the value of the SCLOG variable.
- 18. Display the file named by the SEGG variable, and identify the entry that relates to your last an command. Is user9 or the root user identified as the user who became user3?
- 19. As the user root, attempt to log in to your partner's system by using the telmer command. Was your attempt su cessful? What massage appears?

 On your partner's system, edit the /etc/default/login file, and change the line that reads:

CONSOLE=/dev/console

so that it reads:

#CONSOLE=/dev/console

- 21. As the root user, again attempt to log in to your partner's system by using the tellnet command. If your login attempt is successful, exit the tellnet session. If not, check the change you made in Step 20, and the again.
- 22. As the root user, attempt to use the ftp command to access your partner's system. Were you successful? Ask your partner to edit the /etc/ftpd/ftpusers file and comment out the root entry. Attempt to use the ftp command to access your partner's system again. List some files in the /tmp directory from the ftp> prompt.
- 23. As the root user, attempt to use the riogin command to access your partner's system. Were you successful? Ask your partner to create a /.rhosts file and enter the name of your system on a line by itself. Attempt to use the riogin command to access your partner's system again.



Exercise: User Access (Level 3)

In this exercise, you complete the following tasks:

- Log failed login attempts
- Use the commands finger, last, rusers, su, and who and
- Examine the suleq file
- Change the /etc/default/legin file to allow rest legins from any terminal
- Change the /etc/ftpd/ftpusers file to allow FTP access as the root user
- Create a /. Thests file to allow root access from another system.

Preparation

This lab requires two systems that list each other in their /etc/inet/hosts files. It also requires two specific users, usex9 and user3, on both systems. Both users should use the password 123pass. Refer to the lecture notes as necessary to perform the steps listed.

Task Summary

In this exercise, you accomplish the foll wing:

- Create the file /var/adm/leginleg. Use the command-line login to make five failed login attempts. List the contents of the /var/adm/leginleg file. Use the finger command to display information for user9 on both your system and your partner's system.
- Use the last command to identify when the first root log:nsession
 on your system occurred and how long the session lasted. Use the
 last command to learn when your system last booted. Use the
 rusers command to list the users logged in on all systems on your
 network and on just your partner's system.

- Use the su command to change your user identity from the root user to user9, both with and without the (dash) option. Record the differences. Use the whoami and who am i commands to list your effective and real user identity during your su sessions. Locate the su log declared in the /etc/default/su file, and identify which user initiated your su attempts.
- As the root user, altempt a session to your partner's system by using the relnet command. Record error messages. Change the CASOLE variable on your partner's system to allow root logins from any terminal. Altempt the relnet session again.
- As the root user, altempt to use the ftp command to access your partner's system. Change the /e-wo/ftpd/ftpusers file to allow root access to your partner's system.
- As the root user, alternot to use the rlogin command to access your partner's system. Ask your partner to create a / , rhos to file that lists your system name. Attempt to use the rlogin command to access your partner's system again.

Tasks and Solutions

Complete the following steps:

1. Log in as the root user, and open a terminal window. Change the directory to /var/acm.

cd /var/adm

- 2. Use the toxed command to create a file called loginlog. (Ensure permissions are set to read and write for the root user only.) If necessary, set the group ownership to sys.
- # touch loginlog
- 4 chard 600 logintog
- # charp sys logislog
 - Log out. From the CDE Options menu, select the Command Line Login option. When the CDE login screen clears, press Return to obtain the command-line login prompt.
 - 4. Enter root after the login pompt, but supply an incorrect password. Do this five times. After the fifth attempt, the CDE login screen appears again. Log in as root, and open a terminal window.

5. Examine the /vax/acto/109inlog file. What does it contain?
This file should contain a list of failed logic attempts which appear similar.

to the following:
login:/dev/pus/2:Tue Dec 18 13:29:22 2001

- 6. Use the finger command to display information for the user called user9. What is the difference in output between the finger -m command and the finger command with no option?
- # finger user9
- # finger -m user9

The finger command with no option lists all user accounts that have the string user in their names and comment fields. The finger - a command lists only the entry for the user named user).

- 7. Use the tinger command to display information for the same user on your partner's system. (You will need to reference your partner's system on the command line.) Try this with and without the un option. Does the -noption change the output that the finger command displays?
- # finger user 90 metreme
- # finger -m usec9@hostname

No.

Use the last command to display login and system reboot activity.
 When did the first root legin occur, and how long did that session last?

last

This information depends on the activity on your particular system.

9. Use the last command to display only system boot activity. When did the system last reboot?

last reboot

This information depends on the activity on your particular system.

- Use the rusers command to list information about the users on all systems on your network segment.
- # CUSECTS -1
- 11. Use the runers command to list information about the users on your partner's system. When, and on what terminal, did the first user listed log in?
- # rusers -1 hostnere

This beformation depends on the activity on your particular system.

12. Switch your user identity to that of usez9. Do not use the - (dash) option.

su user9

\$

13. Display some of the variables that define your environment.

- \$ echo \$LOZNAME
- S echo SHOME

Are the values reported correct for the user root or for users?

14. Exit the su session and try to switch your user identity again, this time using the = (dash) option.

\$ axit

su - user9

5 echo \$LOQUE

\$ echo \$BURR

Are the values reported now correct for the user root order user?

 Use the whomai and who am i commands to list your effective and real user identity.

\$ /usr/ucb/wheani

\$ who am i

What do these commands report?

The /usr/ucis/wholen's command displays the login name matching your effective UID, users. The who am i command displays the login name matching your real UID, root.

16. Use the su command to change your user identity from user9 to user3, and use the whomai and who am i commands again.

\$ su user3

235890-5: 123pagg

\$

What do these commands report?

\$ /usr/ucb/whoami

user3

\$ who am i

reet.

Exit both suscessions when you are finished.

3 exit

5 extit

ä.

17. Change the directory to /etc/default. Examine the /etc/default/su file, and record the value of the SUEDS variable.

od /etc/default

more eu

/war/adm/sulog

18. Display the file named by the SULOG variable, and identify the entry that relates to your last su command. Is users or the root user identified as the user who became users?

cat /var/adm/sulog

roct

19. As the zoot user, aftern pt to log in to your partner's system by using the zolinet command. Was your attempt successful? What message appears?

telnet hostname

(telnet connection messages)

SunCS 5.9

legin: root Password: cangetin

The login attempt should not succeed. It fails and the system sends the messages:

Mot on Aystem console Commestion closed by fereign hest.

20. On your partner's system, edit the /etc/default/login file, and change the line that reads:

CONSOLE=/day/console

so that it reads:

#CCNSCLE=/der/console

21. As the root user, again attempt to log in to your partner's system by using the telnet command. If your login attempt is successful, exit the teinet session. If not, check the change you made in Step 20, and try again.

telnet host

(telnet connection messages)
SumOS 5.9

login: root

Password: cangetin

Last legin: Fri Feb 8 08:38:17 fnom sys41

Sun Microsymtems Inc. SumOS 5.9 s81_54 May 2002

* coit

Contraction closed by foreign hest.

22. As the root user, attempt to use the ftp command to access your partner's system. Were you successful?

No, you should receive the message: Login incorrect. Login tailed.

Ask your partner to edit the /etc/ftpd/ftpusers fileand comment out the root entry. Attempt to use the ftp command to access your partner's system again. List some files in the /tmp directory from the time prompt.

You should see files such as:

didocache_: 0

stitvolcheck402

speckeysd.lock

23. As the root-user, attempt to use the rloginguomand to access your partner's system. Were you successful?

You should not be able to use the xlogin command to directly access your parties a system. You should be prompted for a password.

Ask your partner to create a / .rhosts file and enter the mame of your system on a line by itself. Attempt to use the *Login currenal to access your partner's system again.

You should be able to use the xlogin command to log directly in to your partner's system now.

Exercise Summary



Discussion - Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercises.

- Experiences
- Interpretations
- Conclusions
- Applications



Restricting Access to Data in Files

After you have established login restrictions, the next task is to control access to the data on the systems. Of course, some users need to be allowed to read various files; other users need permission to change and delete files, and there are some files that no regular user should be able to access.

Users who need to share files should be in the same group in the /eco/group file.



Note - In general, you use file acress permissions to determine which users or groups have permission to read, modify, or delete files.

Determining a User's Group Membership

The groups command displays group memberships for the user.

The command format for the groups command is:

Groups (Deetmann)

For example, to see which groups you are a member of, perform the command:

i groups

other root bin sys adm utop mail try lp nutop daemon

To list the groups to which a specific user is a member, use the groups command with the user's name, such as user's, as an argument.

groups user5

staff class sycadmin

Identifying a User Account

You use the ideommand to further identify users by listing their UID number, user name, GID number, and group name. This information is useful when you are troubleshooting file access problems for users.

The 1d command also returns the EUID number and name, and the EGID number and login name. For example, if you logged in as user 1 and then used the su command to become user 4, the i d command reports the information for the user 4 account.

The command format for the id command is:

id opcions usernaus

To view your effective user account, perform the command:

S 3d

uid=101(user1) @id=300(class)

To view account information for a specific user, use a viser login name with the id command:

\$ id user1

uid=101 (userl) gid=300(clmss)

To view Information about the secondary groups of a user, use the -a option and a user login name, such as user1:

\$ id -a user1

uid=101(user1) gid=300(class) groups=14(sysamin)

Changing File and Directory Ownership

You might need to use the chown command to change the original owner of a file or directory to another user account on the system. By default, only the root user can change the ownership of a file or directory.



Note – Regular users can be given permission to use the chown command to change the ownership of files and directories owned by them. Edit the /etc/system file, and add the parameter: set_rstchment0 (zero). You need to reboot the system for the changes to take effect.

The command format for the chown command is:

chown option(s) user_nume filename(s)

OT

chown Pation(s) UID filename(s)



Note - The user must exist in the /etc/passwd file.

In this example, a user named user1 created a file called file7.

```
# cd /export/home/user1
# ls -1 file7
-rw-r--r- 1 user1 staff 672 Jun 1 15:11 file7
```

You can use the circum command to give ownership of this file to a new user named user 2. You use the 1s command to verify the new ownership.

```
# chown user2 file7
# ls -1 file7
-rw-r--r-- 1 user2 staff 672 Jun 1 15:22 file7
```

After this sequence of commands, the file is owned by user 2. This file is still in the none directory of user 1. The two users need to determine if the file should be moved to a new directory location.

The owner aby subdirectories can be changed in the same manner as files, as shown in the following examples:

In this example, user I owns a directory called dirt.

You would use the chosen command with the -Reption to give ownership of this directory and all of its contents (files and subdirectories) to use 2.

5 chown -R user2 dir4 \$ ls -lR dir4 dir4: tetal 0 -IW-Y--Y--1 user2 staff 0 Mar 19 16:06 file1 -<u>Y</u>-1/1-<u>Y</u> -- Y --1 userZ sta.ff 0 Mar 19 15:06 file2 -rw-r---1 user2 statf 0 Mar 19 16:06 file3

The -R option makes the chown command recursive. It descends through the directory and any subdirectories, setting the concrehip UID number as it moves through the directory hierarchy.

The chean command can also change both the individual and group cornership of a file or subdirectory simultaneously.

\$ chown neer3:class file2

Additionally, you can use the -R option to descend a directory hierarchy recursively, changing individual and group ownership of the directory and its contents simultaneously. The following example demonstrates this kind of change to the directory.

```
$ chown -R user3:class dir1

$ ls -IR dir1

dir1;

tetal 0

-rw-r--r- 1 user3 class 0 Mar 19 15:18 file1

-rw-r--r- 1 user3 class 0 Mar 19 16:18 file2
```

Changing File and Directory Group Membership

The charge command can be used by the root user or the file's owner to change the group ownership of files and directories to another group on the system. However, the file owner must also belong to the new group.



Note - Regular users can be given permission to use the charge command to change a file's or directory's group ownership to groups of which the user is not a member. Edit the /ekc/system file, and add a parameter: set rstchem=0 (zero). You must reboot the system for the changes to take effect.

The command format for the carry command is:

chgre greupname filename(s)

or

chgrp GID filename(s)



Note - The groupname must exist in the /etc/group file.

For example, the file of file currently is a member of a group named staff.

la -l file4

-re-ra-r- 1 userl Staff

√874 Jun 1 15:08 €

file4

You would use the charp command to give this file to a new group named class and use the 1s command to verify the new group ownership.

f chgrp class file4 # 1s −1 file4

-EW-ZW-Y-- 1 user1

use:1 class

874 Jun 1 15:09

file4

When you are finished, all users who are members of the group called class have read and write access to this file.

Using File Permissions

Three types of special permissions are available for executable files and directories. These are:

- The metuid permission
- The setgid permission
- The Sticky Bit permission

The setuid Permission on Executable Files

When the set-user identification (setuid) permission is set on an executable file, a user or process that runs this executable file is granted access based on the owner of the file (usually the root user), instead of on who started the executable.

This setting allows a user to access files and directories that are typically accessible only by the owner of the executable. Note that many executable programs must be run by the root user or by sys or bin to work property.

Use the 1s command to check the setuid permission.

1s -1 /www/bin/su

-r-sr-xr-x 1 rect

C9.20

22292 Jan 15 17:49 /usr/bin/su

The secraid permission displays as an "s" in the owner's execute field.



Note - If a capital "S" appears in the owner's execute field, it indicates that the setwidbit is on, and the execute bit "x" for the owner of the file is off or denied.

The react user and the owner can set the setuid permissions on an executable file by using the chood command and the octal value 4 ###.

For example:

chmod 4555 executable file

Except for those semiid executable files that exist by default in the Solaris OE, you should disallow the use of setulid programs or at least restrict their use.

To search for files with setuid permissions and to display their full path names, perform the command:

find / -perm -4000

The setgid Permission on Executable Files

The set-group identification (setgid) permission is similar to the setuid permission, except that when the process runs, it runs as if it were a member of the same group in which the file is a member. Also, access is granted based on the permissions assigned to that group.

For example, the write program has a setgid permission that allows users to send messages to other users' terminals.

Use the 1s command to check the setgid permission.

1s -1 /usr/bin/write

-Y-XY-SY-X 5 mo-

rtv

11484 Jan 15 17:55 gusz/bin/write

The setted permission displays as an "s" in the group's execute bold.



Note — If a lowertase letter "1" appears in the group's execute field, it indicates the the setgid bit is on, and the execute bit for the group is off or denied. This indicates that mandatory file and record locking occurs during file access for those programs that are written to request locking.

The root user and the owner can set set gid permissions on an executable file by using the canonic command and the octal value 2# ##. Here is the command-line format:

chmod 2555 executable file

The sengial Permission on Directories

The setgid permission is a useful feature for creating shared directories.

When a setgid permission is applied to a directory, files cronted in the directory belong to the group of which the directory is a member.

For example, if a user has write permission in the directory and creates a file there, that file is a member of the same group as the directory and not the user's group.

To create a shared directory, you must set the setteric bit using symbolic mode. Here is the format for that mode:

chood gts shared_directory

To search for files with setgid permissions and display their full path nances, perform the command:

find / -perm -2000

Sticky Bit Permission on Public Directories

The Sticky Bit is a special permission that profesh the files within a publicly writable directory.

If the directory permissions have the Sticky Bit set, a file can be deleted only by the owner of the file, the owner of the directory or by the most. user. This prevents a user from deleting other users' the from publicly writable directories.

Use the 1s command to determine if a directory has the Sticky Bit permission set.

it ls -ld /tmp

invironment 6

root

719 May 31 03:30

The Sticky Bit displays as the letter "t" in the execute field for other.



Note - If a capital "T" appears in the execute field for other, it indicates that the Sticky Bit is on; however, the execute bit is off or denied.

The reserrand the owner can set the Sticky Bit permission on directories by using the chroad command and the octal value 1 ## #. Here is the command-line format:

chmod 1777 public_directory

To search for directories that have Sticky Bit permissions and display their full path names, execute the following command:

find / -type d -perm -1000



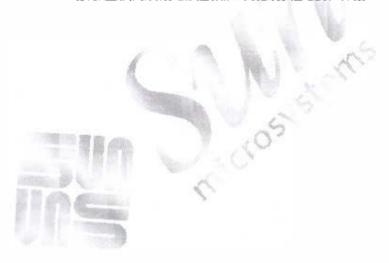
Note - For more detailed information on the Sticky Bit execute the man sticky command.



Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guidance. Each bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab provides more guidance. Although
 each step describes what you should do, you must determine the
 commands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because each step provides exactly what you should input to the system. This level also includes the task solutions for all three levels.



Exercise: Restricting Access to Data on Systems (Level 1)

In this exercise, you complete the following tasks:

- Practice using commands related to user identity and file ownership.
- Assign a user to the sycadmin group
- Assign special file permissions to files

Preparation

Refer to lecture notes as necessary to perform the steps listed.

Tasks

Com lete the following tasks:

Using the commands presented in the lecture, identify the groups of which rect is a member. Compare the output from these commands. Add a user account called user11 with the useraild command. Verify the list of groups of which user11 is a member. Use the Solaris Management Console to create a new user account called user12. Add user11 to the systemin group.

(Steps 1-7 in the Level 2 lab)

• Log in as special and create a new file called file. Attempt to change its recordens by. Record error messages thang the group ownership of file! to sysachin. Switch the user identity to the root user, and change ownership of file! to user!?

(Steps 8-11 in the Level 2 lab)

As user'll, create a new file calle file2. Set setuid and setgid
permissions on file2. Remove all execute permissions from file2.
Record the permissions listed as you damge them.

(Steps 12-15 in the Level 2 lab)

• Record the permissions associated with the /tmp directory. As useril, create a new file called tescl in the /tmp directory. As user12, alternpt to remove this file. Record the result. As user11, create a new directory called dirl in /export/none/user11. Set permissions for the dirl directory to 777. Create a file called test2 in the dirl directory. As user12 attempt to remove this file. Record the result. Log in again as the root user.

(Steps 15-21 in the Level 2 lab)

Exercise: Restricting Access to Data on Systems (Level 2)

In this exercise, you complete the following tasks:

- Practice using commands related to user identity and file ownership.
- Assign a user to the sysachula group
- Assign special file permissions to files

Preparation

Refer to lecture notes as necessary to perform the steps listed.

Task Summary

In this exercise, you accomplish the following:

- Using the commands groups, i.e., and i.e., identify the groups of which the root user is a member. Compare the output from these commands. Add a user account called user11 with the useracid command. Verify the list of groups of which user11 is a member. Use the Solaris Management Console to create a new user account called user12. Add user11 to the sysadmin group.
- Log in as user11 and create a new file called file1. Attempt to change its user ownership. Record error messages. Change the group ownership of file1 to sycadmin. Switch your user identity to the root user, and change ownership of file1 to user12.
- As useril, create a new file called file2. Use the chmod command
 to set setuid and setgid permissions on file2. Use the chmod
 command to remove all execute permissions from file2. Record the
 permissions listed as you change them.
- Record the permissions associated with the /true directory. As user11, create a new file called test1 in the /true directory. As user12, attempt to remove this file. Record the result. As user11, create a new directory called dir1 in /toport/home/user11. Set permissions for the dir1 directory to 777. Create a file called test2 in the dir1 directory. As user12 attempt to remove this file. Record the result. Log in again as the most user.

Tasks

Complete the following steps:

- Log in as the root user, and open a terminal window. Use the groups command to display the groups of which root is a member. Record the list that the groups command displays.
- 2. Use the id. command both without and then with the -a option-

Does the id command report the primary or a secondary group for the root user?

Compare the id -a command output with that from the groups command in Step 1. What additional information does the id -a command provide?

 Use the useradd command to create a new user account called user11 with the following characteristics:

User Name: userll
User ID: 1011
Primary Group: 10
Login Shell: Korn

Home Directory: /export/home/user11

Comment: SA239 User Password: 123pass

- 4. List the groups of which userll is a member.
- 5. Open a terminal window, and launch the Solaris Management Console.

 Open the User Accounts tool. Select Add User from the Action menu. Then select From Template. Create a user account from the following information. Exit the Solaris Management Console when you are finished.

User (D: 1012

Cassword: 123Pass

- From a terminal window, use the usermod command to add user11 to group 14. Verify that the change took place. Log out.
- 8. Log in as user11. Open a terminal window, and use the touch command to create a file called file1. Verify that user11 and the group staff own file1.
- Alternpt to change the owner of filel from user'll to user'll.
 What error message displays?
- 10. Attempt to change the group ownership of file! from staff to systemin. While thange. Did it work?
- 11. Switch your user identity to the root user, and change the directory to /export/home/user11. Change the owner of file1 from user11 to user12. Verify the change. Did it work? Exit your suscession when you're found.
- 12. In the home directory for user 11, use the touch command to create a filecalled file2. Display and record the permissions associated with file2.
 - 13. Use the direct command to add setuid and execute permissions to file?. Display and record the permissions associated with file?. What changed?
 - 14. Use the chood command to add settlid and settlid permissions to file2. Display and record the permissions associated with file2. What changed?
 - 15. Use the chrodiominand with ortal arguments to remove all execute permissions from £1 le2. Display and record the permissions associated with £2.02. What changed?
 - 16. Change the directory to / (root), and list the permissions associated with the /topp directory. Is the Sticky Bit set on /axx? Do all users have write permission in the /axx directory?

- 17. Change the directory to /trp. Create a file collect rest1 in the /trp directory. Verify that user11 and the group staff own rest1 and that 644 (rw-r-r-) permissions apply. Do they?
- 18. Switch your user identity to user12. In the /tap directory, attempt to remove the test1 file. What messages appear? Exit your su session when you are finished.
- 19. In the home directory for userili, create a directory called 6irl. Change permissions for the dirl directory to 777. Create a file called test2 below the dirl directory.
- 20. Switch your user identity to user12. Attempt to remove the file test2 from the dir1 directory. Verify that the test2 file no longer exists. Exit your su session when you are finished.
- 21. Log out, and log in again as the root user.



Exercise: Restricting Access to Data on Systems (Level 3)

In this exercise, you complete the following tasks:

- Practice using commands related to user identity and file ownership.
- Assign a user to the sysacmin group
- Assign special file permissions to files

Preparation

Refer to lecture notes as necessary to perform the steps listed.

Task Summary

In this exercise, you accomplish the following.

- Using the commands groups, id, and id—a, identify the groups of which the root user is a member. Compare the output from these commands. Add a user account called object by using the useradal command. Verify the list of groups of which user11 is a member. Use the Solaris Management Console to create a new user account called user12. Add user11 to the sysadmin group.
- Log in as user IT and create a new file cailed file1. Attempt to change its user ownership, Record error messages, Change the group ownership of file1 to sysachoin. Switch your user identity to the root user, and change ownership of file1 to user12.
- As user11, create a new file called file2. Use the chinod command to set setudd and secgid permissions on file2. Use the chinod cummand to remove all execute permissions from file2. Record the permissions listed as you change them.
- Record the permissions associated with the / and directory. As user11, create a new file called test1 in the / and directory. As user12, attempt to remove this file. Record the result. As user11, create a new directory called dir1 in /exper1/home/user11. Set permissions for the dir1 directory to 777. Create a file called test2 in the dir1 directory. As user12 attempt to remove this file. Record the result. Log in again as the record user.

Tasks and Solutions

Complete the following steps:

 Log in as the root user, and open a terminal window. Use the groups command to display the groups of which root is a member. Record the list that the groups command displays.

groups

other noot bin sys adm uncp mail thy lp twoop darmon

2. Use the ideomorphic both without and then with the -a option.

14

Does the id command report the primary or a secondary group for the root user?

The id command reports the primary group.

id -a

Compare the id -a command output with that from the groups command in Step 1. What additional information does the id -a command provide?

The 12 - a command reports group ID numbers in addition to group names for all groups.

 Use the useradd command to create a new user called userill with the following characteristics:

User Name: user11
User ID; 1011
Primary Group: 10
Login Shell: Rorm

Home Directory: /expout/home/userll

Password:

Comment: SA239 User

useradd -u 1011 -g 10 -d /emport/home/user11 -m -s /bin/ksh -c "SA239 User" user11

123pass

64 blocks

passwd userll

New password: 123pass

Re-enter new password: 123pane passwd (SYSTEM): passwd successfully changed for user11

4. List the groups of which userll is a member.

id -a userll

staff.

5. Open a terminal window, and run the Solaris Management Console.

smc &

6. Open the User Accounts tool. Select Add User from the Action Inchu. Then select With Template. Create a user account from the following information. Exit the Solaris Management Console when you are firished.

User ID: user12

Password: 123pass

From a terminal window, use the userred command to add user? 1
to group 14. Verify that the change took place. Log out.

usermod -G 14 user11

id -a userl1

- Log in as user11. Open a ferminal window, and use the bouch command to create a file called Sile1. Verify that user11 and the group staff own file1.
- \$ touch file!
- \$ 1s -1 file1
- 9. Attempt to change the owner of file! from useril to user!2. What error message appears?
- \$ chown user12 File)

chor: filel: Not cover

- 10. Attempt to change the group ownership of fillel from staff to sysadmin. Verify the change. Did it work?
- \$ charp sysamin file1
- \$ 1s -1 file1

Yes.

Switch your user identity to the root user, and change the directory
to /export/bone/user11. Change the owner of filel from user11
to user12. Verify the change. Did it work? Exit your susession when
you are finished.

```
$ su =
Password: cangetin
# pwd

/
# cd /export/home/user11
# chown user12 file1
# 1s =1
-rw-r--r- 1 user12 sysadmin 0 Apr 17 2002 file1
# exit
```

Yes.

- In the home directory for user11, use the couch command to create a file called file2. Display and record the permissions associated with file2.
- 5 touch file2
 \$ ls -1 file2

The permissions for file2 should read -rw-r--r.

13. Use the chined command toward setude and execute permissions to file2. Display and record the permissions associated with file2. What changed?

\$ chuod 4555 file2 \$ 1s -1 file2

The permissions for file2 should rend -r-sr-xr-x.

- 14. Use the chined command to add setuid and setgic permissions to file2. Display and record the permissions associated with file2. What changed?
- \$ chmod 6555 file2
 5 ls -1 file2

The permissions for file2 should read -r-sr-sr-x

15. Use the chmod command with octal arguments to remove all execute permissions from file2. Display and record the permissions associated with file2. What changed?

\$ chmod 6444 file2
\$ ls -1 file2

The permissions for file2 should read -r-Sr-Ir--.

16. Change the directory to / (root), and list the permissions associated with the / and directory. Is the Sticky Bit set on the / and directory? Do all users have write permission in / and?

\$ cd / \$ ls -1d tmp

Yes to both.

- 17. Change the directory to /tmp. Create a file called test1 in the /tmp directory. Verify that user11 and the group staff own test1 and that 644 (rw-r--r-) permissions apply. Do they?
- \$ cd targo
- \$ touch testI
- \$ 1s -1 test1

YUS.

18. Switch your user identity to user 2. In the /com directory, intempt to remove the Less 1 file. What one sages appear? But your xix session when you are finished.

\$ sw user12
Password: 123pass
\$ rm test1

nn: nest1: override protection 644 (yes/no.) y

nn: cest1 not rangued: Paralasion depied
\$ extit
\$

- 19. In the homedirectory for user11, create a directory called direct. Change permissions for the dir1 directory to 777. Create a file called test2 below the dir1 directory.
- \$ cd
- 3 mkdir dirl
- \$ chmod 777 dirl
- S touch dirl/test2
 - 20. Switch your user identity to user12. Attempt to remove the file test2 from the Girl directory. Verify that the test2 file no longer exists. Exit your su session when you are timished.

\$ su user12 Password: 123pass \$ rm dir1/test2 \$ 1s -1 dir1 \$ exit

21. Log out, and log in again as the root user.

Exercise Summary



Discussion - Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercises.

- Experiences
- Interpretations
- Conclusions
- Applications



Configuring Printer Services

Objectives

Upon completion of this module, you should be able to:

- · Identify network printing fundamentals
- Configure printer services
- Administer printer services
- Start and stop the line printer (LP) print service:

The following course map shows how this module fits into the current instructional goal.

Managing Network Printers and System Processes



Figure 12-1 Course Map

Introducing Network Printing Fundamentals

The Solaris Operating Environment (Solaris E) IP print service provides a complete printing environment that allows the sharing of printers across systems and a set of software utilities that enable users to print files while they continue to work on other tasks.

Print Management Tools

The LP print service software contains the following components for the set up and administration of printers in the Solaris,OE:

- Solaris OE Print Manager A graphical user interface (GUI) that provides the ability to configure and manage printers.
- LP print service commands A command-fine interface that configures and overages printers. These commands also provide functionality not available in the other printmanagement tools.

Client-Server Model

The Solaris OE print service is implemented in a dient-server model.

Print Server

A print server is any system that is configured to manage a printer directly configure to it or that is attached to the network. The print server makes the printer available to other systems on the network and prevides specifing for the client's print requests.

Print Client

A print client is a system that sends paint requests to a print server.

Types of Printer Configurations

As a system administrator, you must configure printers so that users have access to one or more printers.

You should distribute printers over several print servers. If one print server becomes unavailable, print requests can be quickly and easily routed to other print servers on the network.

The Solaris OE supports local, network, and remote printer configurations.

Local Printer

A local printer is physically connected to a system and is accessed from that system.

Network Printer

A network printer is physically attached to the network and has its own host name and truemet Protocol (IP) address. A network printer provides print services to clients but is not directly geometred to a print server.

Remote Printer

A remote printer is one that use reacce. sover the network, that is, a printer that is either physically connected to a remote system or physically attached to the network.

Figure 12-2 shows the concept of local, network, and remote printers.

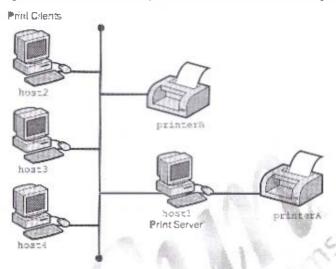


Figure 12-2 Local, Nietwork, and Remote Printers

The printer named printers, connected to the system named hostl, is a local printer for any user logged on to that system.

The printer named parinterB is a network printer that is controlled by the print server, rost1. This is a network printer for any users logged in on host1, host2, host3, or host4.

For users who are logged in to host2, host3, or host4, both printerA and printerS can be accessed as remote printers.

Basic Functions of the Solaris OE LP Print Service

Basic functions of the Solaris OE LP print service include initialization, queuing, tracking, fault notification, and filtering.

Initialization

The Solaris OELP print service initializes a printer prior to sending it a print request. The initialization function ensures that the printer is in a known state.

Queuing

The Solaris ©E LP print service quotes the point requests. The queuing function schoolies the print requests that are waiting to be sent to the printer.

Tracking

The Solaris OE LP print service tracks presents of every print request. The tracking function enables the root user to manage all of the requests and typical users to view or cancel their own requests. This function also logs any errors that have occurred during the printing process.

Fault Notification

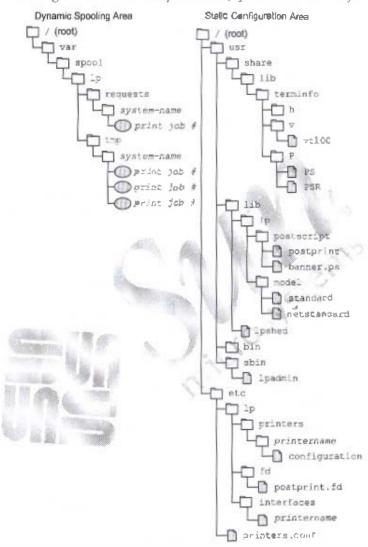
The Solaris OE LP print service provides fault notification if a problem occurs in the print service. The fault notification function prints an error message on the console or sends an email to the good user, depending on how the ser-life has been configured.

Filtering

The Solaris OE LP print service provides filtering capabilities that convert point jobs to the appropriate type of file for the destination printer.

LP Print Service Directory Structure

The Solaris OELP print service includes a directory structure, files, and logs. The following section describes some of the more important components of this structure.



See Figure 12-3 for an example of the LP print service directory.

Figure 12-3 LP Print Service Directory Structure

The /usr/bin Directory

This directory contains the LP print service user commands, such as the lp, 1pstat, and cancel commands.

The /usr/sbin Directory

This directory contains the LP print service administrative commands, such as the ipadmin, ipasers, and ipabut commands.

The /usr/share/lib/tenminf Directory

This directory contains the terminfo database directories, which describes the capabilities of printers and terminals.

The /usr/lib/lp Directory

This directory contains the apsched daemon, binary files that the LP print service uses, PostScript if ters, and standard printer interface programs. Two important subdirectories in the /usr/lib/lp directory are the model and postscript directories.

The /usr/lib/ip/model Directory

This directury contains two default printer interface programs or shell scripts, called the standard and the netstandard scripts.

The standard script supports total printers. For example, when a print request is queued for printing, the print service runs the printer's standard script to:

- Initialize the printer port, if necessary
- Initialize the actual printer, using the termines database to find the appropriate control sequences
- Printa banner page, if necessary
- Print the correct number of copies, as specified by the user's print request

The recestance of script specifically supports network printers. It colleds the spooler and print database information needed to perform network printing and passes the information to a print output module. The nexpermodule opens the network connection to the printer and sends the data to the printer.



Note - The netpr module is located in the /usr/lib/lp/bin directory.

The root user can modify any printer's interface script. For example, to turn off the printing of a banner page, edit the /eto/lp/interfaces/Printer_name file on the print server. Change the nobanner line from:

nobanner="no"

lic

rushamer="yee"

The /usr/lib/lp/pestscript Directory

This directory contains all PostScript filter programs pruvided by the Salans OE LP print service.



Note - Print filters are programs that the print server uses to convert the content type of a queued print request from one format to another format that is acceptable to the destination printer.

The PostScript print filters in this directory handle many situations in which the printer requires the content of files to be in PostScript format.

These filters have companion descriptor files in the /etc/lm/fd directory that tell the LP print service the characteristics and location of the filters.

The /stc/19 Directory

This directory contains a hierarchy of LP server configuration directories and files.

You can view the contents of these configuration files. However, you should not edit these files directly. To make configuration changes, use the lpadmin command or printing? GUL

There are three subdirectories in the /emc/lp directory that are important to printer configuration. There are the fd, interfaces, and printers directories.

 The /etc/lp/fd directory contains a set of print filter descriptor files. These files describe the characteristics of the filter and point to the actual filter program.



Note - The /etc/lp/filter.table file contains a filter lookup table.

- The /eto/lp/interfaces directory contains each printer's interface script file. When a printer is configured, the print service places a copy of the appropriate default interface script from the /wsr/lib/lp/model directory into the /etc/lp/interfaces/printermane file. The printername variable is the file created that contains the n-wly configured printer's own interface script.
- The /=mo/lp/printers directory contains a subdirectory for each printer served by the system. Each subdirectory contains configuration information and alert files for an individual printer.

For example, the configuration file for a printer named printerB can contain the following information:

cat /etc/lp/printers/printerB/configuration

Banner: optional

Content types: postscript

Device: /dev/null

Interface: /usr/lib/lp/model/n tstandard

Printer Spic PS

Modules:

Options: dest=princers, protocol=isso

The /var/spool/lpDirectory

This directory contains a list of current requests that are in the print dueue.

The ipsched daemon for each system keeps track of print requests in the following directodes:

- /var/sccol/lp/tmp/system-name
- /var/symol/lp/requests/system-mane

Configuring Printer Services Copyright 2003 Sun Microsystems, Inc. All Alghis Reserved, Sun Services, Florvision Ag With a local print request, the /var/spool/lp/tmp/system-runne directory contains one file, and the

/var/spool/lp/requests/system-name directory contains another file.

With a remote print request, the /var/spool/lp/r-mp/system-name
directory contains two files, and the
/var/spool/lp/requests/system-name directory contains one file.

- Only the root user or 1p users can access the information in the /var/spool/1p/requests/system-name directory.
- Only the user who submitted the print request, the root user or the LE user can access the information in the /var/spool/lp/Orp/system-name directory.

These files remain in their directories only as long as the print request is in the quoue. After completing the print request, the print service combines the information in the files and appends it to the /v-m/lp/logs/requests file.



Note - The /var/spool/print directory contains the client-side request staging area for the LP print series.

The /war/lp/logs Directory

This directory contains an ongoing history of print requests. The log file /var/1p/logs/requests contains information about completed print requests that are no longer in the print queue.

The /usr/sbin/injetd Internet Service Daemon

The Internet services daemon, inetid, is the server process for many network services. It is usually started up at system boot time. The daemon listens for tervice requests on the ports that are associated with each of the services listed in its configuration file, /ete/inetd.conf. When a request arrives, the inetid daemon executes the server program that is associated with the service. Print servers listen for print requests with the inetid daemon, and upon hearing a request, start up the intid daemon.

The /usr/lib/print/in.lpdProgram

The ineed daemon starts the in. 19d program, sometimes referred to as the protocol adapter. The in. 19d program implements the network listening service for the print protocol. The print protocol provides a remote interface that enables systems to interact with a local spooling system. This protocol defines standard requests from the print client to the print server, such as requests to start queue processing, to transfer print jobs, to retrieve print status, and to cancel print jobs.

Upon the receipt of a connect request, the in, lpd program starts and services the connection. The in lpd program closes the connection and exits after servicing the request.

The /usr/lib/lp/lpsched Daemon

The LP print service has a scheduler daemon called 1950hed. The scheduler daemon updates the LP system files with information about printer setup and configuration. It also manages requests issued to the system by the LD and lpr commands.

The Insched daemon schedules all of the local print requests on a print server. It also tracks the status of printers and filters on the print server. When a printer finishes a request, the Insched daemon schedules the next request, if there is one in the queue on the print server.

Each print server has by default only one lpsched daemon running. It is started by the control script /etc/rc2.d/s\$01p when the system is booted (or enters run level 2). The parent lpsched daemon spawns a child lpsched processes to service print jobs.

Solaris OE Printing Process

Users submit print requests from print clients by using the 1p or 1px commands.



Note - The Solaris OE Print Service accepts both the System V Interface Definition (SVID) /usr/lein/lp command and the Berkeley Software Distribution (BSD) /usr/ucb/lpr command to submit print requests.

Users should use these commands to print text files. These commands do not print documents created in applications such as FrancMaker. Most third-party applications require you to print from a selection mean within the application.

The function of the 12 and 1pr commands is to queue print requests for printing on a destination printer.

Locating the Destination Printer

The Solaris OE LP print service checks several resources to locate the destination printer for a print request.



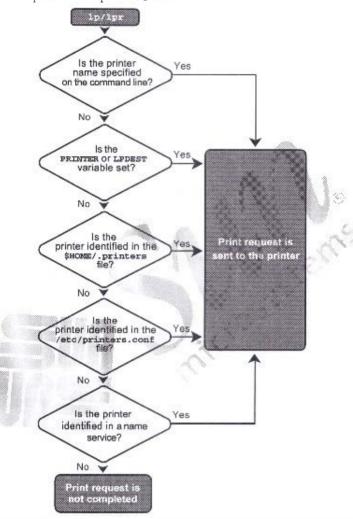


Figure 12-4 shows the resources checked as it identifies the appropriate printer for a print request.

Figure 12-4 Locating the Destination Printer

If the command line does not specify a named printer destination, the user's shell environment is checked.

You can set the LPIST or PRINTER environment variables to a default printer name. The 1p command checks LPIST and then PRINTER. The 1pr command reverses the order when searching for a printer.

If neither variable specifies a named printer destination, then the Solaris **©**E LP print service checks for the variable named _default in the following files:

• The SHOME/ printers file

Users can create their own . Printers file in their home directory to set the default printer name. They should add the following line to the file:

_default printername

If the SHUME/, printers file does not exist or does not specify a printer name destination, then the Solaris OE LP print service checks the /elc/printers.conf file.

• The /etc/printers.conf file

Each entry in the /etc/printers.comf file describes a printer destination. For example, if boot1 is the print server's name and printers is the printer's name, the entry in this file appears as follows:

default:\

: use=printerA: \

printerA:\

| badaddr=hegga, printerA, Selaris | description=printerA

If the _me fault variable is not set, then the _default variable in the name service distabase (for example, Network Information Service (NIS)) is checked.

• The printers . cor. f . Dynamo he

The printers.conf. Dyname file is the NIB version of the /acc/printers.conf file. In this case, the _default variable entry in the name service map called printers.conf. byname defines the print server and printer name destination.

default: hsdaddr=servern ame, printername:

If the destination printer name cannot be located in any of these configuration resources, the print request cannot be completed.



Note - The last three files described in the following paragraphs rely on the printers: entry in the NIS version of the /etc/nsswitch.comf file.

An example of the /etc/ns=witch.conf file syntax is:

printers: user files nis

where:

user = macks \$HOME/.printers f: e files = Checks /etc/printers.conf file nis = Checks printers.conf .byname file

Introducing the Local Print Process

When a user submits a print request to a local printer, the 1p or 1pr command sends the request to the 1psched daemon. The 1psched daemon is also called the print scheduler.



Configuring Printer Services
Copyright 2003 SUN Microsystems, Inc. All Rights Reserved. Sun Services, Revision A.2

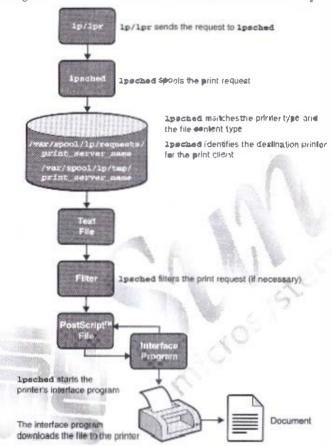


Figure 12-5 shows the role of the 1000 mediaermen in the printing process.

Figure 12-5 Local Printing Process

The losched daemon matches the printer type and identifies the default printer for the system. It then filters the print job.

The 19 sched darmin keeps track of print requests in the following directories:

- /var/spoul/lp/requests/system name
- /var/spmil/ip/tmp/system_name

If the printer is free, the losched daemon starts the printer's interface program. The interface program performs the following functions:

- Initializes the printer port
- Initializes the printer
- Prints the baruter page
- Prints the correct number of file copies
- Sends any fault notifications

Remote Print Process

When a user submits a print request to a remote printer, the lp or lpr command sends the print request directly to the print server.

The print server processes the print request and sends the print request to the destination printer to be printed.



Figure 12-6 shows a remote print request submitted from a print client to a print server in the Solaris OE.

Figure 12-6 Solaris OE Remote Printing

The client's print command communicates directly with the print service on the server to transfer a print request to the printer.

The print server listens for print requests with the Internet services daemen inetd. When the inctd daemen hears a request for a print service on the network, it starts the in.lpd program. The in.lpd program is also called the print pretocol adapter. The in.lpd program starts on demand and exits when the network request finishes.

The print protocol adapter translates the print request, communicates it to the print specier, and returns the results to the print requester.

The print profinced adap to contacts the <u>Insched daemon</u> to start the printer's interface program and to transfer the print request to the destination printer.

Configuring Printer Services

Configuring printer services in the Solaris OE involves a number of key tas s. Table 12-1 shows these tasks.

Table 12-1 Main Tasks for Configuring Printer Services

Tasks	Description	
Setting up the printer	Physically connecting the printer to a system or the network	
Setting up the print server	Configuring the system that is to manage and provide access to the printer	
Setting up the print client	Configuring the system to access a remote printe	
Verifying printer access Checking that the print server recognizes all paint client recognizes the print server.		



Note—When a network of systems is not running a name service, such as NIS, enter each print server's host name and IP address in the lead/inet/fibsts file on the print client when you are setting up the printer services.

Identifying Print Server Requirements

Any system on the network can be a print server if it has the resources to manage the printing load, such as spooling space and memory.

Spooling Space

The spooling space is the amount of disk space that is used to store and process print requests. Spooling space is the most important factor to consider when designating systems as print servers. The recommended starting size (or spooling space is from 25 to 500 Mbytes, depending on the typ—and the size of files being printed and the number of users.



Note - The term spool is an acronym for system peripheral operation offline

Memory

The Solaris OE requires 64 Mbytes of memory to run on a system. Print servers do not require additional memory. However, an extra 32 Mbytes of memory can improve performance when the server is filtering print requests.

Using the Solaris OE Print Manager

The Solaris OE Print Manager enables you to set up and manage printers.

The Solaris OE Print Manager is the preferred method for managing printers. When used with a name service such as NIS, it centralizes printer information and simplifies printer administration.



Note – The Solaris OE Print Manager recognizes existing printer information on print servers, print clients, and in the name service databases.

The following steps demonstrate how to configure a network printer with the Solaris Print Manager. As the root user, start the Solaris OE Print Manager with the following command:

/usr/sach/achin/bin/printmgr &

You can also start the Solaris OE Print Manager by selecting the Printer Administrator from the Tools option on the Common Desktop Environment (CDE) Workspace menu and entering the host name of the workstation to continue.

Fither method displays the Solaris OB Print Manager main window, with Figure 12-7 overlaid on top of it.



Figure 12-7 Select Naming Service Window

Click OK to select the default, files.
 Figure 12-8 remains on the screen.

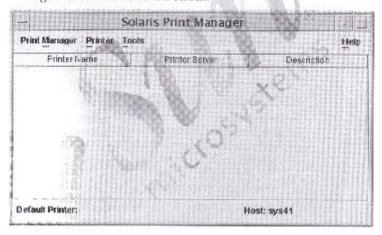


Figure 12-8 Solaris OE Print Manager Window

2. Click the Printer menu in this window. Figure 12-9 shows possible menu selections on the Printer menu.

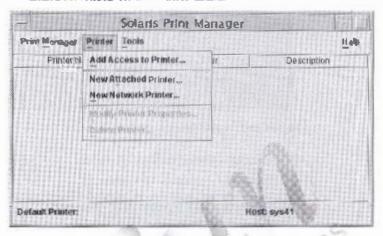


Figure 12-9 Solaris O.F. Print Manager Grister Menu



Note — By clicking Print Manager and selecting Show Command Line Console, you can see the command-line equivalents to each of the actions taken to configure printers. You can then save these steps as commands to perform similar actions in the future or build your own scripts for configuring printers.

Menu selections include:

- Add Access to Printer Selected from a print client to set up access to printers that are controlled by a print server. The host name and IP address of the print server must be in the print client's /etc/inet/hosts file or in a name service database (for example, NIS).
- New Attached Printer Selected from a print server to configure a printer that is physically connected to it. The print server provides the queoing capabilities, filtering, and printing administration.
- New Network Printer Selected from a print server to configure a printer that is directly attached to the network. The print server provides the queuing capabilities, filtering, and printing administration. The network printer's name and its IP address must be entered either in the print server's /etc/inet/hosts file or in a name service database.

Configuring a New Network Printer

Table 12-2 shows the information you would use to configure the new network printer.

Table 12-2 Information Fields for Configuring a New Network Printer

Required Field	Des ription		
Printer Name	A unique name for the network printer. The name can contain a maximum of 14 alphanumeric characters, including dashes and underscores. This is the name entered on the command line with a print command.		
Printer Server	Defaults to the name of the system on which you are currently running the Solaris OE Print Manager. This system is the print server for this network printer.		
Descripti e n	Thispield is optional. A printer's description commonly contains information to help users identify the printer (for example, physical location or printer type).		
Printer Type	The generic name for the type of printer (for example, PostScript, HP Printer, Diablo). The LP print service identifies each printer by its printer type. Printer type data is held in the direct ry /usv/share/lib/terminfo. The Other option, located at the end of the list, allows for the selection of any other printer type listed in the teaminfo database.		
File Contents	Specifies the data format of files that can be printed without any special filtering by the LP print service software.		
Fault Notification	The list of choices for how the superuser is notified of printer errors. These include: Write to Superuser, Mail to Superuser, or None.		

Table 12-2 Information Fields for Configuring a New Network Printer (Confinued)

Required Field	Description	
Destination	The network printer's unique access name. The Destination access name can be either the name of the printer or its IP address as defined in the /etc/inet/hosts file or in a name service detabase. The Destination access name is used only by the print subsys en when it is making the network connection to the physical printer or the printer configuration database and is associated with the network printer's IP address. The internet protocol traits used to communicate with the printer for file transfer. The choices are Berkeley 65D Printer Protocol and raw Transmission Communication of the printer across printers. The printer vendor documentation supplies the information about the protocol to select.	
Protocol		
options	Identifies two options, the Default Printer option and the Always Print Banner option, which by default, are disabled. To enable an option click in the appropriate box (a check mark appears).	
User Access List	Specifies print clients that can print to this printer. By default the word all allows every print client access to this printer.	

From the print server, use the following procedure to set up the configuration information to provide access to a new network printer.

From the Printer menu, select the New Network Printer option.
 Figure 12-10 shows the window that appears.

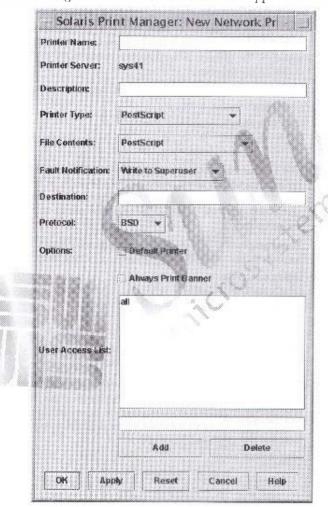


Figure 12-10 Solaris Print Manager: New Network Printer Window

- 4. In the Printer Name field, enter the new printer name, for example,
- Click the Description field, and enter a printer description of your choice.
- For the purposes of this demonstration, accept the default Printer Type: PostScript.

The LP print service uses information in the terminfo database to initialize the printer, as well as to communicate the sequence of codes to the printer.

To view the contents of the terminfo directory, type the following command:

ls /usr/s are/l /terminfo

1 2 3 4 5 6 7 5 9 A a B b c d e f 5 5 H h i j k 1 M n n o 2 p q r S s t u v w x Y z

The terminfo directory contains many different subdirectories that are named with a letter or digit. Use the same initial letter or digit that the manuforturer assigned to the printer's generic name. The terminals and moderns too.

For example, the printer tope for a particular Epson printer would be located in the subdirectory /ust/share/lib/terminfo/e.

H ls /usr/share/lib/terminfo/e

ergo1000 ep2500+h14h exidy 2500 emots epson2500 ep2500+1cw env230 esprit envision230 epv0 epson2500-80 ethernet ep2500+basigy €₽4000 epson2500-hi മ്പ3000 ep2500+colo ep4089 epson2500-hi80 exicy

7. Accept the default File Contents: PostScript.

Every printer has configuration information pertaining to the content type of files that it can accept for its printer type. The LP print service depends on this configuration information to match the numberal type of each print request to the printer type, which ensures that the file is printed correctly. By selecting a file content ty e, as shown in Table 12-3, you can specify the data format of the file that can be priorted without any special filtening by the print software.

Table 12-3 Descriptions of File Content Types

File Content Type	Description	
ASCII	ASCII files do not require filtering.	
PostScript	PostScript files do not require filtering. PostScript is the default.	
Both PostScript and ASCII	PostScript and ASCII files do not require filtering.	
None	All files require filtering, except those matching the printer's type.	
Any	No filtering required. If printer cannot handle the file content type, the file is not to be printed.	

- 8. Click Fault Notification, and select the Mail to Superuser option.
- 9. Click the Destination field, and type a Destination access in me.

If the network printer is not recognized by it name or IP address in the hoste table, you might need to use the vendor-supplied access name for the network printer, which is sometimes qualified by a designated port number. These are both explicitly defined in the printer vendor's documentation.



Table 12-4 shows the format for a Destination entry.

Table 12-4 Destination Entry Format

Destination	Protocol
printer_name	BSD
system_name:printer	BSD
IP_ADDR	BSD
IP_ADDR:port_number ¹	TCP
printer_node_name:port_number	TCP _

- The port number is print server dependent. For example, LexMark uses
 Port 9100.
- 10. Leave the Internet protocol set to BSDE
- 1]. Click in the Default Printer box to enable the Default Printer option.



Note - If coabled, the Default Printer option designates this printer as the default printer for print jobs from this system.

- You can (optionally) click to the Always Print Banner box to enable the Always Print Banner option.
- 13. Accept the default, all, for the Oser Access List. This allows all users on all systems to use the printer.

To restrict user access to this prin er, you can enter the values shown in Table 12-5 in the text field below the User Access List window.

Table 12-5 User Access Values

Value	Definition	
user-name	The specified user, for example user1, can access the printer from any system.	
system- name!user-name	The specified user from the named system can access the printer, for example, host2!user4.	
mystem-name!all	All users from the named system only can access the printer, for example, host5!all.	
all/usor-name	The apacified user from all systems can access the printer, for example, all!user1.	

Note - To delete an entry from the User Access List, select the entry, and dick Delete.





 To accept the new network printer's configuration information, click OK.

Figure 12-11 shows the Solaris OE Priot Manager window, which is displaying the newly configured printer.

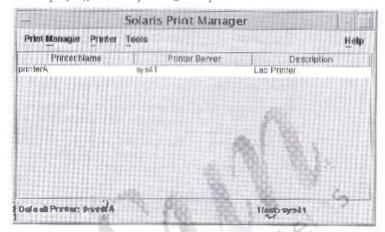


Figure 12-11 Solaris OE Print Manager Window: Configured Printer

 To close the Solaris OE Print Manager window, select the Exit option from the Print Manager menu.



Administering Printer Services

You use the lead min command to configure the LP print services from the command line.

You could use this command to perform the following tasks:

- Defining printer devise, and printer names
- Specifying interface programs (custom or standard) and printer options
- Defining printer types and file content types
- Creating printer classes
- Defining allow and deny user lists
- Specifying fault recovery
- Removing printers and printer classes

The pacenin command is most commonly used by the root user for the purpose of:

- Creating printer classes
- Setting or changing a system's default printer destination
- Removing a printer's configuration from the LP print service

Configuring Printer Classes

You can increase printer access by establishing printer classes. A printer class is a way of grouping individual printers so that they can be identified by a single name known as a class name.

After a printer class is created, you use it as the destination for users' print requests. The LP print service automatically sends each print request to the first available printer within the class that matches the content type expected by the printer. This useful feature can help you balance the load of print requests among several printers.

A printer class can include:

- Specific printer types (for example, all PostScript printers)
- Printers in a specific location (for example, Building 2)
- Frinters in a specific work group or department (for example, Marketing, Engineering, Accounting).

You can create a printer class by using the Leadern command only on the print server for which the printers are configured. Printer classes cannot be defined on print clients.

Configuring Printer Priority Within a Class

When you create a printer class, the root user can control the printer access order by adding the printers to the class in a descending order. For example, by adding a high-speed printer to the printer class first, you can enable it to handle as many print requests as possible, before off-loading to the printer that wand doed to the class next, and so on.

Creating a Printer Class

You create a printer class when the first printer is added to the printer class name. After creating a printer class, you can add other printers to it at any time.

The following example creates a printer class called toldga:

lpadmin -p printerB -c bldg2

The following example adds another printer (printerD) to this class:

1padmin -p printerp -c bldg2

After you have finished adding printers to the printer class, use the accept command to allow quantizing of print requests to the new print queue (p1692 in the example).



Note - The accept command is explained in Module 13, "Using Print Commands."

accept bldg2

destination "bldg2" now accepting requests

Use the lost at let command on the print server to check the status of the new printer class:

1pstat -t

scheduler is coming system default destination: printerA members of class bldg2: printerB printerB

device for printerB: /dev/null
device for PrinterD: /dev/null
bldg2 accepting requests since Fri Jan 4 10:37:44 MST 2002
printerP accepting requests since Fri Jan 4 10:37:44 MST 2002
printerP accepting requests since Fri Jan 4 10:37:44 MST 2002

To send a print request to a printer class, perform the following command:

t lp -d bldg2 myfile

request id is bldg2-0 (1 file)

Setting the System's Default Printer

The root user can run the Ipacmin command to set an individual printer or a printer class to be the system's default destination for all print requests.

- # lpadmir. -d printername
- # Ipadoin 6 printer-classmane

For example, to set a system's default destination printer, perform the command:

lpadmin -d printerE

To verify that the system's default destination printer has been set, perform the command:

lpstat -d

system default destination: printers

To verify an individual user's default destination printer, perform the command:

\$ 1pstat -d

system default destination: weers printer

The print request issued is sent by default to printerE.

1p myfile

request id is printerE-514 (1 file)

Changing the System's Default Printer Class

To change a system's default destination printer to the class b1692, perform the command:

- # lpadmin -d bldg2
- Ť

‡ lpstat -d

system default destination: hldq2



Note – You cannot activate or deactivate a printer class with the enable and disable commands. You can activate or deactivate only the individual printers within a printer class. But you can allow or disallow spooling a classes' jobs by using the commands accept and reject. The commands enable, disable, accept, and reject are explained in Module 13, "Using Print Commands."

Removing a Client's Printer Configuration

To remove a printer's configuration manually on the client side, perform the following:

- I. Log in as the root user on the print client that has access to the printer to be removed from the LP print service.
- Delete information about the printer from the print client by performing an lpachain command.
- # lpadmia -x prinsermame

where -x deletes the specified printer.

For example, the following command deletes printerD from the system.

lpadmin -x printerD

Information for the specified printer is deleted from the print client's /eto/spinters.conf file.

Repeat Steps 1 and 2 for each print client that has access to the printer.

Removing a Server's Printer Configuration



Note - The reject and clisable commands are explained in Module 13, "Using Print Commands."

To remove a printer's configuration manually on the server side, perform the following:

- Log in as the root user on the print server on which the printer is configured.
- 2. Stop queuing print requests on the printer.
- # reject printerD
 - 3. Stop the printer.
- # disable printerD
 - 4. Delete the printer from the print server.
- + leadmin -x printerD

This action deletes configuration information for the printer from the print server's /etc/lp/printers directory and /etc/printers.comf file:

Starting and Stopping the LP Print Service

The LP print service is started by the Insched daemen and is shut down by the Isshut command.

Starting the LP Print Service

The Ipsched doesnon starts or restorts the LP print service. Printers that are restarted with a Ipsiched command from the command line, reprint, in their entirety, the print requests stopped by the Ipsicat command.

The following is an example of starting the libraried daemon from the command line:

/usr/lib/lpsched

Print services started

The 1p print service script, located in the /etc/init.d directory, also can be used to start the 1psched darmon.

/etc/init.d/lp start

Print services started

Stopping the LP Print Service

The Ipshut command stops the LP print service. Any printers that are currently printing when the command is invoked stop printing.

The following is an example of the lashut command:

/usr/lib/lpaint

Print services stopped.

The 1p print service script, located in the /eto/init.d directory, also can be used to stop the 1psched daemon.

/etc/imit.d/lp stop

Print services stopped.

Using Print Commands

Objectives

Upon completion of this module, you should be able to:

- Specify a destination printer
- Use the LP print service

The following ourse map shows how this module fits is to the current instructional goal.

Managing Network Printers and System Processes



Figure 13-1 Course Map

Specifying a Destination Printer

In the Solaris OE, users a brill print requests by using the 1p command or the lar command.



Note - The Solaris OE LI Print Service accepts both the SVID /usz/bin/lp command and the BSD /usr/usb/1_orcommond to submit print requests.

Using the 1pCommand

The 1p command is located in the /usr/bin directory. The 1p command submits a print job to the default printer of to another printer (by specifying the printer name). To use the command, perform one of the following commands:

- \$ /ust/bin/lp filename
- \$ /usr/bin/lp -d printername filename

Using the 1pr Command

The lpr command is located in the /usr/ucb directory. The lpr command functions in the same manner as the 12 command—it submits a print job to the default printer or to another printer.

- \$ /usr/ucb/lpr filename
 \$ /usr/ucb/lpr +P printername filename

The preceding examples of the print commands demonstrate the atomic style. You can also use the Portable Open Systems Interface (POSIX) style to specify a destination printer.

To submit a print request that uses the POSIX style, include the print command and an option, followed by the printer server name, a colon, and the printer name as configured on the printserver.

The full command-line entry is as follows:

- \$ /usr/bin/lp -d hostname:printername filename
- \$ /usr/ucb/lpt -P hostname:printername filename

13.3

Using the LP Print Service

The LP print service is a set of software commands, utilities, and filters that allow users to print files and the root user to set up and manage the print operations.

Table 13-1 lists some of the more commonly used print service administration commands.



Note - You must be the root user to use these commands.

Table 13-1 LP Print Service Administration Commands

Description					
Permits print requests to be queued for the specific printers					
Prevents print requests from being queued for the specific printers					
Activates the sp cificd printers					
Deactivates the specifical timer					
Moves print requests from one printer destination to another					

Accepting Print Jobs

As the root user, you use the accept command on the print server to permit print requests to be guessed on the specified printers.

Using the accept Command

You use the accept command to allow quoting of print requests for the named destinations. A destination specifies the name of a printer or printer class.

The format for the command is:

/usz/sbin/accept destination(#)

Using Print Commands

Capylight 2003 Sun Managers Inc. As Physics Presented. Sun Devilue. Particle A.2

in the following example, the $r\infty r$ user has enabled the queuing of print r que is on printerD.

accept printerD

destination 'printerD' now accepting requests

Rejecting Print Jobs

As the root user, you use the reject command on the print server to prevent print requests from queuing on the specified printers.

Using the reject Command

You use the reject command to prevent print requests from queuing and stop us is from submitting requests to the printer queles.

The format for the command is:

| /usr/sbin/reject =r "reasen" destination(s)

The following example shows how in use the option of "reason" to enter an exploration for the rejection of print requests for a printer. A user charge that text by issuing the Ipstat —a or Ipstat —t command.

reject -r "Replacing Temer Cartridge" printerD
destination "printerD" will no longer ascept requests

Enabling Printers

On the print server, as the root user, you can use the enable command to activate the apprinted printers.

Using the enable Command

The enable command activates the printers, which enables the printing of requests submitted to the print queues.

The format for the command is:

/usr/bin/enable destination(s)

The following example shows how to enable printerp.

anable printerD

printer "printerD" now enabled

Disabling Printers

On the print server, as the root user, you can use the disable command to deactivate the specified printers.

Using the disable Command

The disable command deactivates printers, which disable them from printing print requests usating in the print queues.

By default, any requests currently printing on the printer when the Gisable command is issued are reprinted in the grentirety when the printer is enabled again.

The format for the command is:

/usr/bin/disable -c | -W -= "reser" destination

Table 13-2 shows the options for the disable command:

Table 13-2 Options for the disable Command

Option	Definition	1				
FC W	Cancels the current job and disables the printer. The current job is not printed later.					
-W	Walts until the current job is disabling the printer.	finished before				
· F	Assigns n reason for the disa printer.	bling of the				

The following example shows how to use the disable command with options.

disable -W -r "Printer down for maintenance" printerO printer "printerD" now disabled

Moving Print Jobs

You use the laneve command to move one or all print requests from one printer destination to another printer destination.

Using the Ipnove Command

The format for the 1 move command is:

/usr/sbin/lpmove source_destination target_destination

To move one or all print requests by using the tpmove command, complete the following steps.

- 1. Become the root user on the print server.
- Use the reject command to prevent any further printrequests from being sent to the print queue. This step notifies users that the printer is not accepting requests.
- # reject -r "PrinterC is down for repairs" printerC dextination "printerC" will no longer accept requests
 - 3. Use the loster command to display the print queue to see how many print requests are to be moved. This step is needed to identify print request identification numbers (IDs) only if selected print requests are going to be moved to another printer.

 Use the Ipstat command to verify that the destination printer is accepting print requests.

i lpstat -a printera

printer printerA accepting requestissince The dan 1

- 5. Move the print requests.
 - For example, to move all print requests from printes0 over to printes2, perform the following command:

lgmzve printer& printer&

move in Progress ...

could of a requests moved from printerC to printerA

 For example, to move one or more individual print requests from printerC to printerA, perform the following command:

1gmove printerC-32 printerC-33 printerA

total of 2 requests moved to printerA

6. When printerC, is available again, use the accept command to print jobs to queue to printerC.

accept printerC

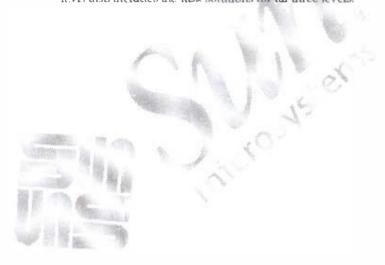
destination "grinters" now accepting requests



Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guldance. Each bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab provides more guidance. Although
 each step describes what you should do, you must determine the
 commands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because each step provides exactly what you should input to the system. This level also includes the task solutions for all three levels.



Exercise: Using the LP Print Service (Level 1)

In this exercise, you use the Solaris **©**E Print Manager to set up a print spiller that sends output to a local terminal window, add access to a remote printer, and use print management commands.

Preparation

The host name and IP address of the system that controls the printer you want to access must exist in the /etc/hosts file. Refer to the lecture notes as necessary to perform the tasks listed.

Tasks

Complete the following tasks:

- Open two terminal windows: Record the pseudo terminal device
 used by one of them. In the other window, run the Solaris OE Print
 Manager, and define a local Diablo printer that asses the first
 window's terminal as its output device. Test the new printer.
 - (Steps 1-7 in the Level 2 lab)
- Use the Solaris OE Print Manager to gain access to a printer defined on another system. Test the remote printer.
 - (Steps 9-13 in the Level 2 lab)
- Manipulate your Diable printer to:
 - Disable printer output
 - Queue four files for printing
- List ali rint jubs
- Cancel two jobs by listing their request IDs
- Cancel the remaining jobs by using their associated user names
- Enable printing again
- Reject print requests and supply a reason
- View the reason
- Accept print requests on the default printer (Steps 14-24 in the Level 2 lab)

Exercise: Using the LP Print Service (Level 2)

In this exercise, you use the Solaris OE Print Manager to set up a print spouler that sends output to a local terminal window, add access to a remote printe, and use print management commands.

Preparation

The host name and IP address of the system that controls the printer you want to access must exist in the /etd/nesta file. Refer to the lecture notes as necessary to perform the tasks listed.

Task Summary

In this exercise, you accomplish the following:

- Open two terminal windows. Record the pseudo terminal device used by one of them. In the other window, run the Solaris OE Print Manager, and define a local Diablo printer that uses the first window's terminal as its output device. Test the new printer.
- Use the Solaris OE Print Manager to gain access to a printer defined on another system. Test the remote printer.
- Use the following commands to manipulate your Diable printer:
 - enable
 - disacie
 - 1p
 - 19sta
 - Accept
 - reject
 - cancel
- Manipulate your Diable printer to:
 - Disable printer output
 - Queue four files for printing
- List att print jobs
- Candel two jobs by listing their request IDs
- Cancel the remaining jobs by using their associated user mannes

- Enable printing again
- Reject print requests and supply a reason
- View the reason
- Accept print requests on the default printer

Tasks

Complete the following steps:

 Log in as the moot user, and open two terminal windows. In one of the windows, use the tay command to identify the pseudo terminal device that it uses. Use this device name as the port for the new printer. For example, the device name in the foll wing tout is identification.

tty /de/z/jets/5

Device name:

- 2. In the other terminal wi dow, run the Solaris OE Print Manager.
- 3. In the Select Naming Service panel, verify that \$\frac{1}{2}\$ less is selected, and click OK. From the Print Manager menu, select the Show Command Line Console option. Position the Command Line Console in a convenient location.
- 4. From the Printer menu, select the New Atta hed Printer option.
- 5. Fillin the fields according to Table 13-3. To name your printer, use a name different from that of your system.

Table 13-3 Configurati n Fields

Field	Selection or Entry				
Printer name	Your choice.				
Oescription Your choice.					
Printer port	Select the Other option. Enter the device name the terminal window found in Step 1.				
Printer type	Diablo.				
File contents ASCII.					
Fault notification Write to superuser.					

Table 13-3 Configuration Fields (Continued)

Field	Selection or Entry				
Default Printer	(Select the box.)				
Always Print Banner	(Do not select the box.)				
User Access List	(No change.)				

- Click WK when you are finished. Notice the command-line entries that appear in the console window.
- Test your printer configuration by printing the /etc/hosts file to the default printer. Observe the output on the other terminal window.
 - You should see the contents of the jest posts file swell through the other window.
- 8. From the Printer menu, select the Add Access to Printer option.
- 9. Fill in the fields according to Table 13-4.

Table 13-4 Configuration Fields

Field	Selection or Entry				
Printer name	Enter the name of a printer on another system.				
Print server	Enter the name of the system on which the proceding printer is defined. Ensure this system name and IP address are in your /etc/hosts file.				
Description	Your choice.				
Default printer	Do not select the box.				

10. Click OK when you are boished.

Notice the commandate entries that appear in the cursole window.

- 11. Test your new configuration by printing the /etc/hosts file to the remote printer. Observe the output on the other syst m.
 - You should see the contents of the /etc/hosts file scroll brough the other window.
- In an available terminal window, use the 1pstat command to display the current status information of the printers on your sys cm.
- 13. Disable print output for your default printer.

- 14. Send the following four files to your default printer: /etc/hosts. /etc/inittab, /etc/dfs/dfstab, and /etc/skel/local.profile.
- 15. Check the print queue to find the request ID for each job.
 The four print jobs should be listed with sequential numbers.
- 16. Use the request IDs to cancel two of the requests. Verify the result. Use the following syntax to cancel the requests:

cancel printername-# printername-#

Two of the print jobs should be gone.

- Cancel the other two jobs by indicating the user who sent them.
 Verify the result.
- 18. Enable printing for your default printer. Use the following syntax:

enable printername

19. Set your default printer to reject requests, and display a reason for doing so. For example:

reject -r "Printer is down for maintenance" printername

 Attempt to send a job to the default printer. Observe the messages displayed.

lp /etc/hosts

Your message should say printername: Requests are not being accept∈d

21. Use the post at command to display the reason that the printer is not according requests. Use the following syntax:

lpstat -a printername

Your message should say printername: Four reason from step 20:

22. Set your default printer to again accept requests.

accept printername

Exercise: Using the LP Print Service (Level 3)

In this exercise, you use the Solaris **©E** Print Manager to set up a print specier that sends output to a local terminal window, add access to a remote printer, and use print management commands.

Preparation

The host name and IP address of the system that controls the printer you want to access must exist in the /eco/hosts file. Refer to the lecture notes as necessary to perform the tasks listed.

Task Summary

In this exercise, you accomplish the following:

- Open two terminal windows. Record the pseudo terminal device used by one of them. In the other window, run to a Solaris OE Print Manager, and define a local Diablo printer that uses the first window's terminal as its output device. Test the new printer.
- Use the Solaris OE Print Manager to gain access to a printer defined on another system. Test the remote printer.
- Use the following commands to manipulate your Diable printer:
 - enable
 - disable
 - lp
 - løstat
 - accept
 - reject
 - espec
- Manipulate your Diable printer to:
 - Disable printer output
 - Queue four files for printing
- List all print jobs
- Cancel two jobs by listing their request IDs
- Cancel tile remaining jobs by using their associated user names

- Enable printing again
- Reject print requests and supply a reason
- View the reason
- Accept print requests

Tasks and Solutions

Complete the following steps:

 Log in as the noot user and open two terminal windows. In one of the windows, use the thy command to identify the pseudo terminal device it uses. Use this device name as the port for the new printer. For example, the device name in the following output is /dev/ets/5:

tty /dev/pts/5

Device: name: Your device nume will vary.

In the other terminal window, run the Solaris OE Print Manager.

/usr/sadm/admin/bin/printmgr &

- In the Select Naming Service panel, verify that files is selected, and click OK. From the Print Manager menu, select the Show Command Line Console option. Position the Command Line Console in a convenient location.
- 4. From the Printer nienu, select the New Attached Printer option.
- 5. Fill in the fields according to Table 13-3 on page 13-11. To name your prime use a name different from that of your system.
- 6. Click OK when you are finished. Notice the command line entries that appear on the console window.
- Test your printer configuration by printing the /etc/hosts file to the default printer. Observe the output on the other terminal printers.

1p /etc/hoets

You should see the contents of the /etic/host.s file scroll through the other window.

13-15

- 8. From the Printer menu, select the Add Access to Printer option.
- 9. Fill in the fields according to Table 13-4 on page 13-12.

Using Print Commands Copyright2003 Stin Microsystems, Inc. All Rights Reserved, Sun Selvices, Revision A.2 10. Click OK when you are finished.

Notice the command line entries that appear in the consule window.

11. Test your new configuration by printing the /etc/flosts file to the remote printer. Observe the output on the other system.

lp -d pristername /etc/hosts

You should see the contents of the /etc/hests file scroll through the other window.

- In an available terminal window, use the 19stat command to display the current status information of the printers on your system.
- # lpstat -t
- 13. Disable print output for your default printer.
- disable printername
 - 14. Sand the following four files to your default printer: /etc/hoses, /etc/inittab, /etc/dfs/dfstab, and /etc/skel/local.profile.
- f lp /etc/hoete
- # lp /etc/inittab
- # lp /eto/dfs/dfstab
- # lp /etc/shel/local.profile
 - 15. Theck the print queue to find the request ID for each job.
- # lpstat -o

The four pair jobs should be listed with sequential numbers.

- 16. Use the request IDs to cancel two of the requests. Verify the result.

 Use the following syntax to cancel the requests:
- # cancel printername-# printername-#
- # 19stat -a

Two of the print jubs should be gone.

- 17. Cancel the other two jobs by indicating the user who sent them. Verify the result. For example:
- T cancel -u root
- # lpstat -o
- 18. Exable printing for your default printer.
- # onable printername
 - Set your default printer to reject requests, and display a reason, for doing so. For example:
- # reject -r "Frinter is done for mintenant" printenant

 Attempt to send a job to the default printer. Observe the messages displayed.

1p /etc/hosts

Your message should say pri termame: Requests are not being accepted

21. Use the lipstat command to display the reason that the printer is not accepting requests. Use the following syntax:

lpstat -a printername

Your message should say printername: your reason from see 20.

22. Set your default printer to again accept requests.

accept printername



Exercise Summary



Discussion – Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercise.

- Experiences
- Interpretations
- Conclusions
- Applications



Controlling System Processes

Objectives

Upon completion of this module, you should be able to:

- View system processes
- Clear frozen processes
- Schedule an automatic one-time execution of a command.
- Schedule an automatic recurring execution of a command

The following course map shows how this module fits into the current instructional goal.

Малаging Network Printers and System Processes



Figure 14-1 Course Map

Viewing System Processes

A process is any program that is running on the system. All processes are assigned a unique process identification (PID) number, which is used by the kernel to track and manage the process. The PID numbers are used by the root and regular users to identify and control their processes.

Using the CDE Process Manager

The Solaris OE Common Desktop Environment (CDE) provides a Process Manager to monitor and control processes that are running on the local system.

To start the Process Manager, click the find Process control on the Tools subpanel of the Front Panel, Figure 14-2 shows the Tools menu.



Figure 14-2 Tools Mcnu

You can also start the CDE Process Manager from the command line by typing the following:

/usr/dt/bin/sdtProcess &

Figure 14-3 shows the window that appears.

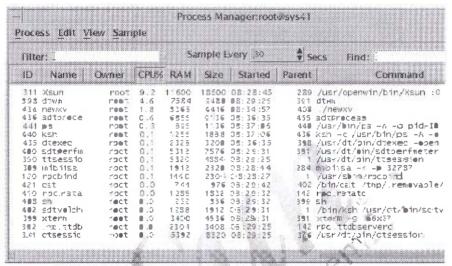


Figure 14-3 CDE Process Manager Window

The Process Manager can sort processes alphabetically (Name) or numerically (ID), depending on the column that is selected.

You can initiate a search by typing text into the Find field.

To terminate a process, highlight it and press Control-C, select the Kill option from the Process menu. or select the kill ption from the options that are available when you press the right mouse button.

Using the prstat Command

The Pristat command examines and displays information about active processes on the system.

This command enables you to view information by specific processes, user identification (UID) numbers, central processing unit (CPU) IDs, or processer sets. By default, the postar command displays information about all processes sorted by CPU usage. To use the postar command, perform the command:

prstat PID USERNAME SIZE RSS STATE PRI NICE TIME CPU PROCESS/NI//P 4600K 4232K CPUO 1257 TOOK 0:00:00 0.3% pretat/1 39 Π 0 0:00:00 0.1% sh/ 328K 256K sleep 59 1243 root 1247 root 1872K 1448K sleep 59 0 0:00:00 0.0% in.telnetd/1 1256 rect 1896K 1416K sleep 49 0 0:40:00 0.0% kah/2 243 IGOT 2840% 2376K sleep 59 0 0:00:00 0.0% nacd/18 2728K 1544K sleep 59 0:00:00 0.0% sand/1 388 FOOL 0 (outgut edited for brevity) 59 C 203 roct 3704K 2032K Sies 0:00:00 0.08 autonoun=0/3 2304E 1392X sleep 228 **root** 59 0 0:05:00 C_0% efcn/l 2848K 2112K 51eap 59 C 1:00:00 0.0% product 59 0 0:00:00 0.0% symmetri/13 62 COSt 2296K 1448K sleep 55 root 2:184K 1368E sleep 132 root Total: 48 processes, 206 lops, load averages: 0.00, 0.00, 0.01

To quit the pretat command, type qu

Table 14-1 shows the column headings and their meanings in a prestat report.

Table 14-1 Column Headings for the acsta; Report

Default Column Heading	Description				
PID	The PID number of the process.				
USERNAME	The login name or UID of the owner of the process.				
SIZE	The total virtual memory size of the process.				
RSS	The rusident set size of the process in kilobytes, megabytes, or gigabytes.				

Table 14-1 Column Headings for the pristat Report (Continued)

Default Column Heading	Description The state of the process: • cpu - The processis running on the CPU.				
STATE					
	sleep - The process is waiting for an event to complete.				
	• run-The process is in the run queue.				
	 zombie - The process terminated, and the parent is no waiting. stop - The process is stopped. 				
PRI	The priority of the process.				
NICE	The value used in priority computation.				
TIME	The cumulative execution time for the process.				
CPU	The percentage of recent CPU time used by the process.				
PROCESS/NLWP	The name of the process/the number of lightweight processes (LWPs) in the process.				



Note — The series and many applications are now multithreaded. A thread is a logical sequence of program instructions written to accomplish a particular task. Each application thread is independently scheduled to run on an LWP, which functions as a virtual CPU. LWPs in turn, are attached to kernel threads, which are scheduled to run on actual CPUs.



Note - Use the priocntl (1) command to assign processes to a priority class and to manage process priorities. The nice(1) command is only supported for backward compatibility to previous Solaris OE releases. The priocntl command privides more flexibility in managing processes.

Table 14-2 shows the options for the prestat command.

Table 14-2 Options for the pretat Command

Option	Description						
-a.	Displays separate reports about processes and users at the same time.						
-c	Continuously prints new r ports below previous reports.						
-п пргос	Restricts the number of output lines.						
-p pidlist	Reports only on processes that have a PID in the given list.						
-s key	Sorts output lines by key in descending order. The five possible keys include: coa, time, alze, ras, and pri. You can use only one key at a time.						
-S key	Sorts output lines by key in ascending order						
-t	Reports total usage summary for each user-						
-v exidlist	Reports only processes that have an effective user ID (EUID) in the given list.						
-V midlist	Reports only processes that have a real UTO in the given list.						



Using the Solaris Management Console Process Tool

The Solaris Management Console provides a tool for monitoring and managing system processes. You open the Process Tool by clicking This Computer, and then clicking System Status. Then click Process.

Figure 14-4 shows the Solaris Management Console Process Tool.

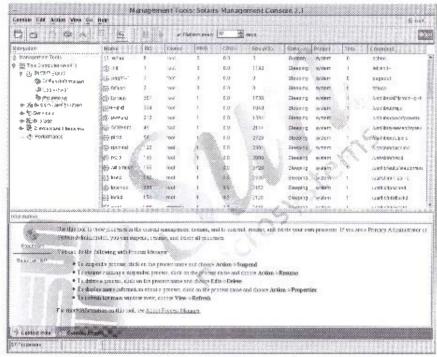


Figure 14-4 Solaris Management Console - Process Tool Window

From the Process Tool, you can do the following:

- Suspend a process. To do this, click the process name, and choose Suspend from the Action menu.
- Resume running a suspended process. To do this, click the process name, and choose Resume from the Action menu.
- Kill (delete) a process. To do this, click the process name, and choose Delete from the Edit menu.
- Display more information about a process. To do this, click the process name, and choose Properties from the Action menu-
- Refresh the main window view. To do this, choose Refresh from the View menu.



Clearing Frozen Processes

You use the kill command or the pkill command to send a signal to one or more running processes. You would typically use these commands to terminate or clear an unwanted process.

Using the kill and pkill Commands

You use the kill or pkill commands to terminate one or more processes.

The format for the kill command is:

kill -signal PID

The formal for the pkill commands:

pkill -signal Process

Before you can terminate a process, you must know its name or PID. Use either the ps or agree command to locate the PID for the process.

The following examples uses the pares command to locate the PID for the mail processes.

```
$ pgrop -1 mail
551 senomail
12047 dimail
$
$ pbill dimail
```

The following examples use the ps and pkill commands to locate and terminate the dtmail process.

```
# ps ~e | grep mail
304 ? 0:00 sendmail
1197 ? 0:01 dtmai|
# %till 1197
```

To terminate more than one process at the same time, use the following syntax:

```
$ kill signal PID PID PID PID
$ pkill signal process process
```

You use the icill command without a signal on the command line to send the default Signal 15 to the process. This signal usually causes the process to terminate.

Table 14-3 shows some signals and names.

Table 14-3 Process Signal Numbers and Names

Signal Numiber	Signal Name	Event	Default Action	
1	SIGHUP	l·langup	Exit	
2	SIGIMT	Interrupt	Exit	
9	SIGKILL	Kill	Exit	
15	SIGTERM	Terminate	Exit	

- 1, STORY A langup signal to cause a telephone line or terminal
 connection to be dropped. For certain decrease, such as inerval and
 in. named, a hangup signal will cause the daemon to reread its
 configuration file.
- 2. SIGNT An interrupt signal from your keyboard—usually from a Control-C key combination.
- 9, SIGKILL—A signal to kill a process. A process carmot ignore this signal.
- 13 SIGTERM A signal to tensinate a process in an orderly manner.
 Some processes ignore this signal.

A complete list of signals that the kill command can send can be found by executing the command kill—, or by referring to the man page for signal:

man -s3hard signal

Some processes can be written to ignore Signal 15. Processes that do not respond to a Signal 15 can be terminated by force by using Signal 9 with the kill or prill commands. You use the following syntax:

- \$ kill -9 PID
- \$ pkill -9 process



Caution - Use the 1611 =9 or pkill -9 command as a last resort to terminate a process. Using the -9 signal on a process that controls a database application or a program that updates files can be disastrous. The process is terminated instantly with no opportunity to perform an orderly shutdown.

Performing a Remote Login

When a workstation is not responding to your keyboard or mouse input, the CDE night be frozen. In such cases, you may be able to remotely access your workstation by using the rlogin command or by using the telnet command from another system.

Killing the Process for a Frozen Login

After you are connected remotely to your system, you can invoke the okill command to terminate the corrupted session on your workstation.

In the following examples, the dog in command is used to log in to 57542, from which you can issue a pkild or a kill command.

S rlogin sys42

Password: EnterPassword

Last login: Mon Jan 14 10:11:56 from sys43 Sun Microsystems Inc. SunOS 5.9 Beta May 2002

\$ pkill -9 Xsun

\$ ps -e | grep Xano

0:03 X.sur 375 ?

s kill -9 379

Scheduling an Automatic One-Time Execution of a Command

Use the attcommand to automatically execute a job only once at a specified time.

Using the at Command

The format for the at command is:

at $-\pi - g$ guduename fime date at -r your at -1

Table 14-4 shows the options you can use to instruct the crop process on how to execut an at job.

Table 14-4 Option for the at Command

Option	Description				
-m	Sends mail to the user after the job has finished				
-r job	Removes a scheduled at job from the queue				
-q queuename	Specifies a specific queue				
time	Specifies a time for the command to execute				
-1 4 7 700	Reports all jobs scheduled for the invoking user				
date	Specifies an optional date for the command to execute, which is either a month name followed by a day number or a day of the week				

For example, to create an all job to run at 9:00 p.m. to locate and delete core tiles from us 12's home directory, perform the command:

я at 9:00 pm

as>find /equat/home/user2 -name dore -emec rm () \; at><Control-D>

commands will be executed using /sbin/sh job 10160%400.a at wed Mar 13 21:00:00 2002

To display information about the execution times of jobs, perform the

at -1 1016078400.a

1016078400.a Wed Mar 13 21:00:00 2002

To display the jobs queue—to run at specified times by chronological order of execution, perform the command:

atg

Rank	Foxecution Date	CANDOR	Job	Queue	Job Name
1st	26am 13, 2002 21:00	root	1016078400.a	a	stdin
2nd	Mar 13, 2002 21:05	roct	1016078700.a	a	stáin
3∠ć.	Mar 13, 2002 21:10	roct	1016079000.a	\a_	stáin

To view all the at jobs currently scheduled in the queue, perform the command:

ls -1 /var/spool/cron/atjobs

-r-Srr- 1	root	other	1	921	Mar	13	13:08	1016078400.a
-r-Srr 1	reet	ozher	4000	913	Plan	13	13:09	101607 \$ 700.a
-r-Srr 1	root	other		885	Var	13	13:03	1016079000 #

You can also use the at orimand to remove a job from the at queue.

For example, to remove job 1016076400, a front the at queue, perform the command:

at -r 1016078400.a

≒ atq

Rank	Executi⊕n Date	Cw::ex	Job	Queue	Job Mame
lst	Mar 13, 2002 21:05	reet	1016078700.∉	а	stdin
2nd	Mar 13, 2002 21:10	root	1016079000.a	වු	stdin

Controlling Access to the at Command

As the root user, you control who has access to the at command with the at. dems and at allow files.

The /etc/cron.d/at.denyFile

By default, the Solaris Off includes the /et.c/cron.d/at.dooy file. This file identifies users who are prohibited from using the at command. The file format is one user name per line. The file initially contains:

daemon bin anto numer listen mebody

A user who is denied access to the set command receives the following message when attempting to use the command:

al: yeu are not authorized to use at. Sorry.

If only the /etc/cron.d/at.demy file exists but is empty, then all logged-in users can access the at command.

The /etc/cron.d/at.allow File

The /etg/cron.d/at.allow file does not exist by default, so all users (except those listed in the /etc/cron.d/at.deny file) can create at jobs. By creating the /etc/cron.d/at.allowfile, you create a list of only those users who are allowed to execute at commands.

The /ero/cron.d/at .allow file consists of user names, one per line.

The interaction between the at.allowand the at.deny files follows these rules:

- If the at. allow file exists, only the users listed in this file can
 execute at commands.
- If the at callow file does not exist, all users, except for users listed in the at .de.by file, can execute at commands.
- If neither file exists, only the root user can use the at command.

Scheduling an Automatic Recurring Execution of a Command

You can use the error facility to schedule regularly recurring commands. Users can submit a command to the error facility by modifying their crontab file.

All crontain files are maintained in the /var/spect/cron/erontains directory and are stored as the login name of the user that created the cron job.

The error daemon is esponsible for scheduling and rurning these jobs.



Note - The clock daemon, cron, starts at system boot and runs continuously in the background.

Introducing the crentale File Format

A cremtab file consists of lines of six fields each. The fields are separated by spaces or tabs. The first five fields provide the date and time the command is to be scheduled. The last field is the full path to the command.



Note - If the command field contains a percent (%) character, then all subsequent chalacters are passed to the command as standard input.

These first five fields are separated by spaces and indicate when the command will be executed. See Figure 14-5.

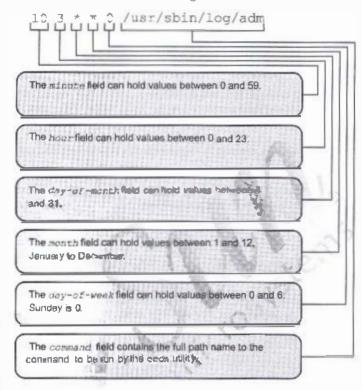


Figure 14-5 First Five Fields in a crontale File

The first five fields follow the format rules shown in Table 14-5.

Table 14-5 Rules for the crontair Fields

Value	Rule	Example	
22	Matches if field value is n	As shown in the preceding figure for hour or minute, a 3 or 10	
n,p,q	Matches if field value is n, p, or g	Every 10 minutes would be represented by 0,10,20,30,40,50	
п-р	Matches if field has values between n and inclusive The hours between 1:00 a.m. and 4:00 a.m. would be represented by		
61	Matches all legal values	As in t e p eceding example for the month, representing every month.	

Using the crontabCommand

The cruntab command enables the user to view, edit, or remove a cruntab file.

Viewing a crontab File

To view the contents of the root crops of file, run the crontab -1 command as the root user.

This is the same command that users run to view the contents of their own crosstab file.

As the root user, you can view the contents of any regular user's crentals file by performing the command:

crontab -1 username

Editing a crontab File

To create or edit a crontabilite, follow these steps:

- 1 Check that the EDITOR variable is set to the editor on want to use. This instructs the even utility which editor to use to open the file.
- # EDITOR=vi
- # export EDITOR
 - 2. Run the following countais command to open your errorters file, and add the appropriate entry.
- # crontab -e

30 17 * * 5 /uer/bin/berner "Time to go!" > /dev/console



Note - If the users do not redirect the sandard output and standard error of their commands in the croncabille, any generated output or errors are mailed electronically to the user.

Removing a crontab File

The correct way to remove a crontab file is to invoke the command:

cruntab -r username

Typical users can remove only their own crontab file. The root user can delete any user's crontab file.



Caution – If you accidently enter the crantaborumand on the command line without an option (-1, -e, -r), press the interrupt key's Control-C to exit. Do not press Control-D; this action overwrites the existing crontab file with an empty file.

Controlling Access to the crontal Command

You can control access to the crontal command with two files in the /etc/crontal directory—the crontality file and the crontality file.

These files permit only specified users to perform or ontall tasks, such as creating, editing, displaying, or removing their own Grontell files.

The /etc/crom.d/crom.deny File

The Solaris OE provides a default oron. deny file. The file consists of a list of user names, one per line, of the users who are not allowed to use oron. The following is an example of the contents of a gron deny file:

daemon bin smtp numcp listen nobody noaccess

The /etc/cron.d/cron.allowFile

The /etc/cron.d/cron.allow file does not exist by default, so all users (except those listed in the cron.deny file) can access their crontab file. By creating a cron.allow file, you can list only those users who can access crontab commands.

The file consists of a list of user names, one per line.

The interaction between the cronuallow and the cronuceny files follows these rules:

- If the cron.allowfile exists, only the users listed in this file concreate, edit, display, or remove crontab files.
- If the cron.allow file does not exist, all users, except for users listed in the error.deny file, can create, edit, display, or remove error tabfiles.
- If neither file exists, only the root user can run the crossbab command.

Using the Solaris[™] Management Console Job Scheduler Tool

The Solaris^M Management Console contains a Scheduled Jobs tool to create and schedule jobs on your system. Users can manage jobs if the following conditions exist:

- Their user name appears in the /els/cron.d/cron.allow file.
- Their user name does not appear in the /etc/carm.d/cron.dergfile.
- The /etc/cron.d/cron.allow and /etc/cron.d/cron.dem; files
 do not exist, and You are the root user.

To open the Job Scheduler from the Solaris Management Consolo, click This Computer and then click Service, and finally, click Scheduled Jobs.

See Figure 14-6 for an example of the Solaris Management Console Job Scheduler window.



Figure 14-6 Solaris Management Console - Job Scheduler Window

You can use the Job Scheduler to:

- View and modify job properties
 Select the name of the job in the view pane, and choose Properties from the Action menu.
- Delete a job

 Select the job name and choose Delete from the Edit menu. The root user can delete all jobs. Users can only view and delete their own jobs.
- Add a scheduled job
 theore Add Scheduled Job on the Action menu.
- Enable and disable job logging, and set search paths
 Choose Scheduled Job Policies on the Action menu.



Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guidance. Each bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab provides more guidance. Although
 each stop describes what you should do, you must determine the
 commands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because
 each step provides exactly what you should input to the system. This
 level also includes the task solutions for all three levels.



Exercise: Using Process Control (Level 1)

In this exercise, you use the Process Tool and the pratat command to monitor and kill processes. You create an at job and create an entry in a grontab file.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed.

Tasks

Complete the following tasks:

• Start the Process Tool. Run the pristat command in a window. In a separate window, run the find / command. Make note of the CPU percentages for the find command, as displayed by the pristat command and the Process Tool. Open a third window, and identify the PID of the shell running in it. Use the Process Tool to show the ancestry of the shell process. Use the Process Tool to kill the shell process. Use the Process Tool to send the TERM signal to the pristat process. Exit the Process Tool when you are finished.

(Steps 1-6 in the Level 2 lab)

• Identify the device associated with your current terminal, and display the current time of day. Submit an at job that echoes Test Complete to your current window. Have the job run five minutes from the current time, and submit it to the queue called x. Display the at job in the queue.

(Steps 7-10 in the Levei 2 lab)

 Set the MOITOR variable to vi. Use the crontab command to determine when the logach process is scheduled to run. Use the crontab command to edit the crontab file for the root user. Add an entry that sends the message It works! to your current window five minutes from the current time.

(Steps 11-14 in the Level 2 lab)

Exercise: Using Process Control (Level 2)

In this exercise, you use the Process Tool and the pastat command to monitor and kill processes. You create an at job and orate an entry in a creatab file.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed.

Task Summary

In this exercise, you accomplish the following:

- Start the Process Tool. Run the present commanding window, in a separate window, run the Eind / command. Make note of the CPU percentages for the find command, as displayed by the Present cammand and the Process Tool. Open a third window, and identify the PID of the shell running in it. Use the Process Tool to show the ancestry of the shell process. Use the Process Tool to send the TERM signal to the present process. Use the Process Tool to send the TERM signal to the present process. Exit the Process Tool when you are finished.
- Identify the device associated with your current terminal, and display the current time of day. Submit an at job that echoes Test.
 Complete to your current window. Have the job run five minutes from the current time, and submit it to the queue called x. Display the at job in the queue.
- Set the EDIDA variable to vi. Use the executal command to determine when the logarith process is scheduled to run. Use the executab command to edit the executab file for the root user. Add on entry that sends the message It works! to your current window five minutes from the current time.

Tasks

Complete the following steps:

- Log in as the root user and open a terminal window. Start the Process Tool either by selecting the Find Process option from the Front Panel Tools menu in CDE or by invoking the appropriate command from the command line.
 - In the Process fool display, sort the listing according to CPU#, and change the sample time to five seconds.
- 2. Open a second terminal window, and run the gratat command.
- 3. Position the Process Tool and the window'in which the pretat command is running so that you can observe both simultaneously. In an available window, run the find command to list all files on your system. Observe how the Process Tool and the pretat command display statistics for the find command.
 - What is the maximum percentage of week CPU time used by the find command as it executes?
- 4. Open a third terminal window, and run the pa command to determine the PID of the shell. Record the PID, you find.
- 5. In the Process Tool, locate and select the shell process you identified in the previous step. Select the Show Ancestry option from the Process from in the Process Tool. What is the name and PID of the first process listed?
- 6. Close the Show Ancestry window. Again, select the shell process you identified in Step 4. From the Process menu in the Process Tool, select the Kill option. What happens?
- 7. In the Process Tool, use the Find function to locate the pretat process. Select the Signal option from the Process mean. In the Signal fill-in field, enter the TERM signal, and click OK. What happens to the pratat process? Close the Process Tool when you are finished.
- Identify the device essociated with your current terminal by using the try command, and display the current time of day.
- Submit an at job that echoes Test Complete to your current window. Have the job run five minutes from the current times and submit it to the queue called x.
- 10. Display the at job in the queue.



- 11. Open a new window and set and export the 20 low environment variable to use the vi editor to edit cront ab files.
 - If you are using the **Fo**mme or Kom shell, perform the command:
- # EDITOR=vi
- # export EDITOR

If you are using the C shell, perform the command:

- # setemy EDITOR vi
 - Use the crontab command to view the current crontab file for the root user.
 - 13. When is the logady process actreduled to run?
 - 14. Use the crontab command to edit the crontab file for the root user. Add an entry that sends the message It works! to your current window five minutes from now. For example, if the current time is 10:25, make an entry in your crontab file for the 30th minute of the same hour.

Save the file, and quit the vicedit session. In about five minutes, you should see the result in your window.



Exercise: Using Process Control (Level 3)

In this exercise, you use the Process Tool and the present compand to monitor and kill processes. You create an at job and create an entry in a creatab file.

Preparation

Refer to the lecture notes as necessary to perform the tasks listed.

Task Summary

In this exercise, you accomplish the following:

- Start the Process Tool Run the prestat command in a window. In a separate window, run the first Accounted. Make note of the CPU percentages for the final command, as displayed by the prestat command and the Process Tool Open a third window, and identify the PID of the shell running in it. Use the Process Tool to show the ancestry of the shell process. Use the Process Tool to kill the shell process. Use the Process Tool to kill the shell process. Exit the Process Tool to send the TERM signal to the Distat process. Exit the Process Tool whenever are finished.
- Identify the revice associated with your current terminal, and
 display the current time of day. Submit an at job that echoes Test
 Complete to your current window. Have the job run five minutes
 from the current time, and submit it to the queue called x. Display
 the at job in the queue.
- Set the ECITOR variable to vi. Use the erontab command to determine when the logadin process is scheduled to run. Use the crontab command to edit the crontab file for the root user. Add an entry that sends the message It works! to your current window five minutes from the current time.

Tasks and Solutions

Complete the following steps:

 Log in as the root user, and open a terminal window. Start the Process Tool either by selecting the Find Process option from the Front Panel Tools menu in CDE or by invoking the appropriate command from the command line.

/uar/dt/bin/sdtprocess &

In the Process Tool display, sort the listing according to OPUE, and change the sample time to five seconds.

2. Open a second terminal window, and run the prestat cummend.

prstat

3. Position the Process Tool and the window in which the present command is running so that you can observe both simultaneously. In an available window, run the first command to list all files on your system. Observe how the Process Tool and the present command display statistics for the find command.

What is the maximum percentage of recent CPU time used by the find command as it executes?

This varies according to your system configuration. Some systems might display values in the 20-percent range.

4. Open a third terminal window, and run the ps command to determine the PID of the shell. Record the PID you find.

ps

Your while ameeors here.

5. In the Process Tool, locate and select the shell process you identified in the previous step. Select the Show Ancestry option from the Process menu in the Process Tool. What is the name and PID of the first process listed?

The PID varies. • n systems running the CDE, the first process listed should be /une/at/bin/dtlogin.

6. Close the Show Ancestry window. Again, select the shell process you identified in Step 4. From the Process menu in the Process Tool, select the Kill option. What happens?

The process stops, and the window two longer appears.

7. In the Process T 1, use the Find function to locate the protat process. Select the Signal option from the Process menu. In the Signal fill-in field, enter the TZRM signal, and click OK. What happens to the protat pricess? Close the Process Tool when you are finished.

The Prestat process terminates, and the prompt appears in the soundors in which it ran.

8. Identify the device associated with your current terminal by using the tty command, and display the current time of day.

tty

(semething like /dev/pts/4 should appear

date

(current date/time appears)

9. Submit an at job that echoes Test Complete to your current window. Have the job run five minutes from the current time, and submit it to the queue called x.

 $\frac{1}{2}$ at $-\mathbf{q} \times 13:30$

at> echo "Test Complete" > /dev/pts/# (# is from the tty commend)

at> <Control-D>

commands will be executed using /sbin/sh job 958163400.x at tri May 12 13:30:00 2000

10. Display the at job in the queue.

atq

11. Open a new window and set and export the EDITOR environment variable to use the vi editor to edit crontab files.

If you are using the Bourne or Korn shell, perform the command:

EDITOR=vi

export EDITOR

If you are using the Cshell, perf im the command:

- # setenv EDITOR vi
 - Use the crontab command to view the current crontab file for the root user.
- # crontab -1
- When is the loga disprocess scheduled to run?
 Ten minutes after 3.00 a.m. on all days

14. Use the crontab command to edit the crontab file for the root user. Add an entry that sends the manage It works! to your current window five minutes from now. For example, if the current time is 10:25, make an entry in your crontab file for the 30th minute of the same hour.

tty /dev/pts/#

date

Thu . May 11 10:25:14 POT 2000

crontab -e

Add the following line, but substitute the correct time and terminal device:

39 10 * * * / /==r/bin/e=ho "it works!" > /dev/pts/#

Save the file, and quit the vi edit session. In about five minutes, you should see the result in your window.

Exercise Summary



Discussion – Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercise.

- Experiences
- Interpretations
- Conclusions
- Applications



Performing File System Backups

Objectives

Upon completion of this module, you should be able to:

- Identify the fundamentals of backups
- Back up an unmounted file system

The following course map shows how this module fits into live current instructional goal.

Performing System Backups and Restores

Performing File System Backups

1724

Performing File System Restores Backing Up a Mounted File System With a UFS Snapshot

Figure 15-1 Course Map

Introducing the Fundamentals of Backups

A crucial function of system administration is to backup file systems. Backups safeguard against data loss, damage, or corruption. Backup tapes are often referred to as dump tapes.

Importance of Routine File System Backups

To back up file systems, you copy file systems to removable media, such as a tape. You perform backups on a regular basis to prevent loss of data due to:

- Accidental deletion of files
- Hardware failures
- Problems with re-installations or system upgrades
- System crashes
- System break-ins by unauthorized users, comprumising data integrity
- Natural disas fees



Tape Media Types

able 15-1 shows typical tape media that you can use to store file systems during the backup process. Select media based on the availability of equipment and your preference.

Table 15-1 Tape Media Types

Media Type	Capacity	
1/2-inch reel tape	140 Mbytes (6250 bits per inch)	
1/4-inch cartridge (QIC) ^T cartridge tape	8 Gbytes	
8-mm cartridge tope	40 Gbytes	
4-rum digital audio tape (DAT)2 cartridge tape	24 Gbytes	
DLT ³ 1/2-inch cartridge tape	70 Glytes	
LTO ⁴ cartridge tape	100 Gbytes	

QIC stands for quarter-inch tape.
 DAT stands for digital audic tape.
 DLT stands for digital linear tape.
 LTO stands for linear tape open.

The capacities in the table are approximate. Tape capacity increases with new technology. Check the documentation that comes with the tape device to determine the capacity.

Tape Drive Naming

All tape drives have logical device names that you use to reference the device on the command line. Figure 15-2 shows the format that all logical device names use.

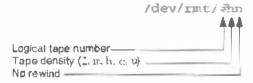


Figure 15-2 Logical Device Name Format

The logical tape numbers in the tape drive names always start with 0. For example:

- The first instance of a tape drive: /dev/mt/0
- The third instance of a tape drive: /dev/rint/2

Two optional parameters further define the logical device name:

- Tape density Five values can be given in the tape device name:

 (low), a (medium), h (high), e (compressed), or u (ultra compressed).
- No rewind The letter n at the end of a tape device name indicates that the tape should not be rewound when the current operation completes.

Tape densities depend on the type drive. Check the manufacturer's documentation to determine the correct densities for the tape media.

Tape drives that support data compression contain internal hardware that aperforms the compression. Hardware compression uses more space than the software compression you can achieve from the Solaris! Operating Environment (Solaris OE) compress command, but compression is much faster. If you back up a software-compressed file with hardware compression, the resultant file is larger in size.

Tape Drive Control

You use the at command (magnetic tape control) to send instructions to the tape drive. Not all tape drives support all at commands.

The format for the maid mmand is:

mt -f tape-device-name command count

You use the -E option to specify the tape device name, typically a no-ressind device name.

Using the mt Command

Table 15-2 lists some of the mt commands that you can use to control a magnetic tape drive.

Table 15-2 Definitions of mt Commands

Command	Definition
mt status	Displays status information about the tape drive
mt rewind	Rewinds the tape
mt offline	Rewinds the tape and, if appropriate, takes the drive unit offline and if the hardware supports it, unloads
mt faf count	Moves the tape forward count records

The following command positions the tape at the beginning of the third tope record.

mt -f /dev/mt/0n fsf 2

Strategies for Scheduled Backups

The most common method to schedule backups is to perform cumulative incremental backups daily. This schedule is recommended for most situations.

In set up a backup schedule, determine:

- The file systems to back up
- A backup device (for example, tape drive)
- The number of tapes to use for the backup
- The type of backup (for example, full or incremental)
- The procedures for marking and storing tapes
- The time it takes to perform a backup.

Determining File System Names to Back Up

Display the contents of the /etc/vfstab Mc. Then view the mount point column to find the name of the file system that you want to back up.

Determining the Number of Tapes

You determine the number of tapes for a backup according to the size of the file system you are backing up.

To determine the size of the file system, use the ufsalo: contonand with the soption. The following are the command formats:

wiedump OS filesyster Wane

⊕ť

f lifedump 35 Filesystem nume <number reporteds

The numeric option determines the appropriate dump level. The output is the estimated number of bytes that the system requires for a complete backup.

Divide the reported bytes by the capacity of the tape to determine how many tapes you need to backup the file system.

Determining Back Up Frequency and Levels

You determine how often and at what level to backup each file system. The level of a backup refers to the amount of information that is backed up.

Identifying Incremental and Full Back Ups

You can perform a full backup or an incremental backup of a file system. A full backup is a complete file system backup. An incremental backup copies only files in the file system that have been added or modified since a previous lower-level backup.

You use Dump Level 0 to perform a full backup. You use Dump Levels 1 through 9 to schedule incremental backups. The level numbers have no meaning other than their relationship to each other as a higher or lower number.

Figure 15-3 shows an example of a fife system backup performed in incremental levels.

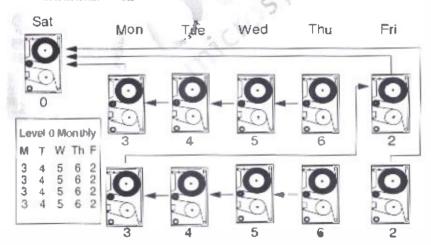


Figure 15-3 Incremental Back Up Strategy

Table 15-3 defines the elements of the incremental backup strategy shown in Figure 15-3.

Table 15-3 Incremental Back Up Level Definitions

Level	Example	
o (Full)	Performed once each month.	
3	Performed every Monday. The backup copies new or modified files since the last lower-level backup (for example, 0).	
4	Performed every Tuesday. The backup copies new or modified files since the last lower-level backup (for example, 3).	
5	Performed every Wednesday. The ackup copies new or modified files a nee the last lower-level backup (for example, 4).	
E	Perfermed every Thursday. The backup copies new or modified files since the last lower-level backup (for example, 5).	
2	Performed every. Friday. The backup copies new or modified files since the last lower-level backup, which is the Level 0 backup at the beginning of the month.	



Note - Many system administrators use the crontab utility to start a script that runs the usedure command.

The /etc/dumpdates File

The /etc/dumpdates file records backups if the -uo tion is used with the ufsdump command. Each line in the /etc/dumpdates file shows the file system that was backed up and the level of the last backup. It also shows the day, the date, and the time of the backup.

The following is an example /etc/dumpdates file.

cat /etc/dampdates

When an incremental backup is performed, the used to consults the /etc/increates file. It looks for the date of the next lower-level backup. Then, the used command copies to the backup media atl of the files that were modified on added since the date of that lower-level backup.

When the backup is complete, the /etc/chmpdates file records a new entry that describes this backup. The new entry coplaces the entry for the previous backup at that level.

You can view the /etc/dumpdates file to determine if the system is completing backups. If a backup does not complete because of equipment failure, the /etc/dumpdates file does not record the backup.



Note – When you are restoring an entire file system, check the /etc/dumpdates file for a list of the most recent dates and levels of backups. Use this list to determine which tapes are needed to restore the entire file system. The tapes should be physically marked with the dump level and date of the backup.

Backing Up an Unmounted File System

Check that the file system is inactive, or unmounted, before you back the system up. If the file system is active, the output of the backup can be inconsistent, and you could find it impossible to restore the files correctly.

The ufseump Command

The standard Solaris OE command for ufs file system backups is /usr/spin/resourg.

The format for the ufsaum command is:

ufsdump option(s) argument(s) filesystem_name

You can use this command to back up a complete or a partial file system. Backups are often referred to as dumps.

Options for the ufscump Command

Table 15-4 defines several common options for the life time command.

Table 15-4 Options or the ufsdum Command

Option	Description	
0~9	Back up level. Level 0 is a full backup of the file system. Levels 1 through 9 are incremental backups of files that have changed since the last lower-level backup.	
v	Verify. After each tape is written, the system verifies the content of the edia against the source file system. If an discrepancies occur, the system prompts the operator to insert new media and repeat the process. Use this option only on an unmounted file system. Any activity in the file system causes the system to report discrepancies.	
ន	Size estimate. This option allows you to estimate the amount of space that will be needed on the tape to perform the level of ackup you want.	
1	Autoload. You use this option with an autoloading (stackloader) tape drive.	
2001	Offline. When the backup is complete, the system takes the drive offline, rewinds the tape (if you use a tape), and, if possible, ejects the media.	
	Update. The system c eates an entry in the /stc/du. The system c eates an entry in the system disk slice, the backup level (0-9), and the date. If an ntry alre dy exists for a ackup at the same level, the system replaces the entry.	
n	Notify. The system sends messages to the terminals of all logg d-in u ers who are members of the sys group to indicate that the ufsdump command requires attention.	
i device		

Tape Back Ups

You use the ufsaump command to create file system backups to tape. The dump level (0-9) specified in the ufsdump command determines which files to back up.

Using the ufsalume Command

Perform the following steps to use the ufedump command to start a tape backup:

 Become the *OOE user to change the system to single-user mode, and unmount the file systems.

/usr/abin/shutdown -y -g300 "System is being shutdown for backup"

Shutdown started. Thu 24 Jan 2002 01:01:47 PM MST

Broadcast Message from root (pting) on hostl Thu Jan 24 01:01:52
The System hostl will be shut down in a minutes
System is being stutden for backup

- Verify that the /export/home file system was unmounted with the shutdown command. If not, unmount it manually.
- 3. Check the integrity of the file system data with the fack command.

fack /export/home

4. Perform a full (Level 0) backup of the /export/name file system.

wishing out /der/met/0 /export/home

```
ufsdamp Ouf /dev/nmt/0 /export/home

DUMP: Writing 32 Kilobyte records

DUMP: Date of this level 0 dump: The 24 Jan 2002 01:06:47 PM MST

DUMP: Date of last level 0 dump: the equals

DUMP: Dumping /dev/rdsk/c0t0d0s7 (host1:/export/home) to /dev/rmt/!!.

DUMP: Mapping (Pass I) [directories]

DUMP: Mapping (Pass II) [directories]

DUMP: Retimoted 1126 blocks (563KB).

DUMP: Dumping (Pass III) [directories]

DUMP: Dumping (Pass IV) [regular files]

DUMP: Tape rewinding

DUMP: 1086 blocks (543KB) on 1 clume at 1803 KB/sec

DUMP: DUMP IS DUME

MIMP: Level 0 dump on The 24 Jan 2002 01:06:47 EM MST
```

Remote Backups to a Tape

You can use the utsatum command to perform a backup on a remote tape device.

The format for the use command is:

ufsdump options remotehost:tapedevice filesystem

To perform remote backups across the network, the system with the tape drive must have an entry in its /, rhoses file for every system that uses the tape drive.

Using the ufsdum Command

The following example shows how to perform a full (Level 1) backup of the /expcrt/none file system on the bos=1 system to the remote tape device on the hos=2 system.

```
# ufsdump Ouf host2:/dev/rmt/0 /export/home
DUMP: Writing 32 Kilobyte records
DUMP: Date of this level 3 dump Tim 24 Jan 2002 01:13:55 PE VST
DUMP: Date of last level 0 dump: the specim
DUMP: Damping /dev/rdsk/c0c3d3s7 (hest1:/export/home) to
host2:/dev/rmt/0

DUMP: Mapping (Pass I) [regular files]
BUMP: Mapping (Pass II) [directories]
DUMP: Inmping (Pass III) [directories]
DUMP: Inmping (Pass III) [directories]
DUMP: Dumping (Pass IV) [regular files]
DUMP: Tape rewinding
DUMP: 318 blocks (159KB) on 1 volume at 691 KB/sec
DUMP: DUMP IS DOME

DUMP: Level 0 dump on Thu 24 Jan 2002 01:13:55 PM MST
```

Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guidance. Each bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab provides more guidance. Although
 each step describes what you should do, you must determine the
 commands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because each step provides exactly what you should input to the system. This level also includes the task solutions for all three levels.



Exercise: Backing Up a File System (Level 1)

In this exercise, you back up an available file system on your system.

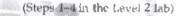
Preparation

This exercise requires a system that is configured with a tape drive and a file system that is available to unmount. This exercise assumes that the /export/home file system exists on a separate partition from the / (mot) like system and can be unmounted. Identify the slice on which the /export/home file system resides. Get a tape that is appropriate for your system from the instructor.

Tasks

Complete the following tasks:

- Use the nt command to resvind the tape to the beginning.
- Use the ufsdum command to create a tage backup of the /export/home file system. Make sure that the /etc/dumpmates file is updated.



- Add files and directories to the /expart/home file system.

 (Steps 5-6 in the Level 2 lab)
- Use the uterdump command to do an incremental backup of the /experimental backup of the

(Steps 749 in the Level 2 lab)

- Use the me command to remove the tape from the tape drive.
- Review the /etc/20000ates file.
 (Steps 10-12 in the Level 2 lab)

Exercise: Backing Up a File System (Level 2)

In this exercise, you back up an available file system on your system.

Preparation

This exercise requires a system that is configured with a tape drive and a file system that is available to unmount. This exercise assumes that the /export/home file system exists on a separate partition from the / (root) file system and can be ramounted. Identify the slice on which the /export/home file system resides. Get a tape that is appropriate for your system from the instructor.

Task Summary

In this exercise, you accomplish the following:

- Use the Et command to rewind the tape to the beginning.
- Use the unstable command to crosse a tape backup of the /export/home file system.
- Add files and directories to the /export/home file system.
- Use the useding command to do an incromental backup of the /export/home file system.
- Use the mt command to remove the tape from the tape drive.
- · Review the /etc/dumpdates file.

Tasks

Complete the following steps:

- Unmount the /export/home file system. If your system reports that
 the /export/home file system is busy, use the amount -- f command.
- 2. Insert a tape into your tape drive.
- Use the mc command to rewind the talle to the beginning.
- 4. Use the ufaduum command to create a backup for the /emont/home file system. Make sure that the /eco/mandates file is updated.
- 5. Mount the /export/name file system.

- Copy the contents of the /etc/unce directory to the /export/home directory.
- 7. Unmount the /export/bane file system.
- 8. Move the tape to the next tape record.
- 9. Use the ufsdum command to create an incremental backup for the /expert/home file system, using a non-rewinding device.
- 10. Rewind and eject the tape from the tape drive.
- 11. Sot the tape aside for use with subsequent labs.
- 12. Review the contents of the /ecc/dampdates file.
- 13. Mount the /expert/home file system.



Exercise: Backing Up a File System (Level 3)

In this exercise, you back up an available file system on your system.

Preparation

This exercise requires a system that is configured with a tape drive and file system that is available to unmount. This exercise assumes that the /export/home file system exists on a separate partition from the / (root) file system and can be unmounted, identify the slice on which the /export/home file system resides. Get a tape that is appropriate for your system from the instructor.

Task Summary

In this exercise, you accomplish the following:

- Use the att command to rewind the tape to the beginning.
- Use the ufacture command to create a tape backup of the /export/home file system.
- Add files and directories to the /export/home file system.
- Use the ufsdump command to do an incremental backup of the /expert/home file system.
- . Use the arc command to remove the tape from the tape drive.
- Review the /etc/dumpdates file.

Tasks and Solutions

Complete the following steps:

Unmount the /export/horse file system. If your system reports that
the /export/home file system is busy, use the unount -f command.

א שישטעה / אויטשע א

- 2. Insert a tape into your to pe drive.
- 3. Use the mt command to rewind the tape to the beginning.

mt rewind

4. Use the afadmin command to create a backup tape for the /export/home file system, where off #a#s# represents. If you cannot remember which device the/export/home file system was mounted on, view the contents of the /etc/vfstab file with the more command.

ufedump Ouf /dev/rdek/c#t#d###

You should see output similar to:

ulsaure out /dev/ntt/0 /dev/rdsk/c0c0t0s7

Dunn: Writing 32 %i obyte records

DUMP: Date of this level 0 drump: Thu 24 Jan 2002 01: 06: 47 FM MST

DUMP: Date of last level C dump; the epoch

DUMIP: Dumping /dev/rds/k/cOtOdOs7 (sys43:/eXport/home) to /dev/rmt/0.

DUMP: Mapping (Pass 1) [regular files]

DLWP: Nepping (Rese II) [directories]

DUMF: Estimated 1125 blocks (563KB).

DUMP: Ownping (Pass I-1) [directories]

DUMP: Dumping (Page IV) Iregular files)

DUMP: Tape rewinding

DEVE: 1096 blocks (541ME) on 1 volume at 1803 KB/sec

DUMP: SUMP IS DONE

DUMP: Level 0 dump on Time 24 Jan 2002 01: 06: 7 PM MST

5. Mount the Yesport/home file system.

& mount / home

 Copy the contents of the /etc/goodirectory to the /export/home directory.

cp -r /etc/uucp /export/home

7. Unmount the /exert/home file system.

T want /wport/home

8. Move the tape to the next tape record.

mt -f /dev/xmt/On fef 1

9. Use the ufsdamp command to create an incremental backup for the /export/home file system, using a non-rewinding device.

i ufedump 1uf /dev/rmt/On /dev/rdsk/c#t#d#s#

You should see output similar to:

ufs@wmp luf /@ev/xmt/On /d@m/rds/k/c@d&t@s? DWR: Writing 32 Kilobyte records

DIMP: Date of this level 0 dump: Thu 24 Jan 2002 01:13:55 FM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DIMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DIMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of this level 0 dump: The 24 Jan 2002 01:13:55 FM MST DUMP: Date of this level 0 dump: The 24 Jan 2002 01:13:55 FM MST DUMP: Date of this level 0 dump: The 24 Jan 2002 01:13:55 FM MST DUMP: Date of this level 0 dump: The 24 Jan 2002 01:13:55 FM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:13:55 FM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:13:55 FM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:13:55 FM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: The 24 Jan 2002 01:06:47 PM MST DUMP: Date of last level 0 dump: Date

DUMP: Dumping /dev/rdsk/c0t0d0s7 (sys43:/expert/home) to /dev/rmt/0.

DUMP: Marring (Pass I) [regular files]

DUMP: Marring (Pass II) [directories]

DUMP: Estimated 320 blocks (160Kb).

MRKP: Dumping (Pass III) [directories]
DUMP: Dumping (Pass IV) [regular files]

COMP: 312 blocks (159KB) on I volume at 691 KB/mac

DUMP IS DONE

DIMP: Level 1 dump on Inu 24 Jan 2002 01:13:55 PM MST

10. Rewind and eject the tape from the tape drive.

† mt offline

- 11. Set the tape aside for use with subsequent labs?
- 12. Review the contents of the /etc/dumidates file.

F mure /etc/duminates

You should see one line showing information for the Level 2 dump and another line for the Level Loung, for example:

/dev/rosk/cGt9d0s7 0 1hm Jan 24 15420:49 2002 /dev/rdsk/c0t0d0s7 1hm Jan 24 13:22:06 2002

13. Mount the /export/have file system.

mount /export/home

Exercise Summary



Discussion - Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercise.

- Experiences
- Interpretations
- Conclusions
- Applications



Performing File System Restores

Objectives

Upon completion of this module, you should be able to:

- Restore uts file systems
- Explain disaster recovery fundamentals

The following source map shows how this module fits into the current instructional goal.

Performing System Backups and Restores

Performing
File System
Backups
Performing
File System
File System
With a UFS
Snapshot

Figure 16-1 Course Map

Restoring a ufs File System

You restore a fle system to rebuild a domaged file system, to reinstall or upgrade the Solaris OE software, or to reorganize file systems on existing or new disks.

Restoring a Regular File System

When you are restoring data to a sys tem, onsider the following questions:

- Can the system boot on its own (tegular file system restore)?
- Do you need to boot the system from CD-ROM (critical file system restore)?
- Do you need to boot the system from CD-ROM and repair the boot drive (special case recovery)?

To restore files or file systems, determine the following:

- The file system back up tapes that are needed.
- The device name to which you will restore the file system
- The name of the temporary directory to which you will restore individual files
- The type of backup device to be used (local or remote)
- The backup device name (loca) or remote)

To restore a regular file system, such as the /export/icome or/opt file system, back disto the disk, you use the ufsrestore command. The ufsrestore command copies files to the disk, relative to the current working directory, from backup tapes that were created by the ufsdump command.

You can use the ugerestore command to reload an entire file system hierarchy from a Lovel C backup and related incremental backups. You can also restore one or more single files from any backup tape.

The format for the afsrestore command is:

ufsrestore option(s) argument(s) filesystem

Table 16-1 describes some options that you can use with the utsrestore command.

Table 16-1 Options for the utsrestore Command

Option	Description
t	Lists the table of contents of the backup media.
r	Restores the entire file system from the backup media.
x file1 file2	Restores only the files named on the command line
i	Invokes an interactive restore.
v	Specifies verbose mode. This mode displays the path names to the terminal screen as each file is restored.
f device	Specifies the tape device name.

When you restore an entire file system from a backup tape, the system creates a restore syntable file. The ufsrestore command uses the restoresyntable file for check-pointing or passing information between incremental restores. You can remove the restoresyntable file whin the restore is complete.

Using the ufsrestore Command to Restore the /opt File System

The following procedure dem strates how to use the ufsrestore command to restore the /ept file system on the c0t0d0s5 slice.

- 1. Create the new file system structure.
- i newfs /dev/rdsk/c0t040eS
 - Mount the file system to the /opt directory, and change to that directory.
- # mount /dev/dsk/c0t0d0a5 /opt
- # ed /opt
- 3. R st re the /opt file system from the backup tape.
- # ufsrestore rf /dev/rmt/0



Note – Always restore a file system by starting with the Level () backup tape, continuing with the next-lower-level tape, and continuing through the highest-level tape.

- 4. Remove the restoresympable file.
- # rm restoresymtable
 - 5. Unmount the new file system.
- # cd /
- # wowat /OPt
- 6. Use the fisck command to check the restored file system.
- # feck /dev/rdak/c0t0d0s5
 - 7. Perform a full backup of the file system.
- # ufsdxrep Ouf /dev/rot/O /dev/rdek/c0t0d0s5



Note — Always back up the newly created like system because the utsrest are command repositions the files and changes the inode allocation.

Restoring the /usr File System

To restore the /usr file system, boot from the Solaris 9 Software 1 of 2 CD-ROM, and then use the ufsrestore command to restore files back to the /usr partition.



Note - If the / (root), /usr, or /var file systems are unusable because of some type of corruption or damage, the system will not boot.

Using the ufsrestore Command to Restore the /usr File System

The following procedure demons rates how to restore the /usr file system on Sice 6 of the boot disk.

- Insert the Solaris 9 Software 1 of 2 CD-ROM, and boot from the CD-ROM with the single-user mode option.
- ok boot caron -s
 - 2. Create the new file system structure.
- # newfs /dev/rdsk/c0t0d0m6
 - Mount the file system to the mount point and change to that directory
- # mount /dev/dek/c0t0d0e6 /a
- i cd /a
- 4 Restore the /usr file system from the backup tape.
- # ufsrestore rf /dev/rmt/0



Note - Remember to resture a file system by starting with the Level 0 backup tape, continuing with the next-lower-level tape, and continuing through the highest-level tape.

- 5. Remove the restoresymtable file.
- # rm restoresymtable
 - 6. Unmount the new file system.
- # cd /
- # unount /a
- 7. Use the isck command to check the restored file system.
- # fack /dev/rdsk/c0t0d0m6
 - 8. Perform a full backup of the file system.
- # uf edump Ouf /dev/rdat/c0t0d0s6
 - 9. Reboot the system.
- # init 6

Performing a Special Case Recovery of the / (root) File System

You perform a special case recovery to recover the / (root) file system if there is damage to the boot block.

To restore the / (root) file system, boot from the Solaris 9 Software 1 of 2 CD-ROM, and use the unsuestage command.

The following procedure demanstrates how to restore the / (root) file system on Slice 0 of the boot disk.

- Insert the Solaris 9 Software 1 of 2 CD-ROM and boot the CD-ROM with the single-user mode option.
- ok boot odran -s
 - 2. Create the new file system structure.
- # newfs /dev/zdak/c0t0d0a0
 - Mount the file system to the mount point /a and change to that directory.
- # mount /de /dsk/c0t0d0s0 /a
- # cd /a
- 4. Restore the / (root) file system from the backup tape.
- # ufsrestore rf /dev/rmt/0



Note – Always restore a file system by starting with the Level 0 backup tape, and continuing with the next-lower-level tape, and continuing through the highest-level tape.

- 5. Remove the restoresymbable file.
- In regumentable
 - Install the bootblk in Sectors 1 through 15 of the boot disk. To do
 this, change to the directory that contains the bootblk, and enter the
 impea! Boot command.
- t cd /usr/platform/'uname -m'/lib/fs/ufs
- installboot bootblk /dev/rdsk/c0t0d0s0
 - 7. Unmount the new file system.
- # cd /
- # umount /a

- 8. Use the #sc's command to check the restored file system.
- # fsck /dev/rdak/c0t0d0s0
 - Perform a full backup of the file system. 9.
- # wfedump Ouf /dev/Int/0 /dev/Idak/cOtOdOsO
 - 10. Reboot the system.
- # init 6

Invoking an Interactive Restore

The ufareatore i command invokes an interactive interface. Through the interface, you can browse the directory hierarchy of the back up tape and select individual files to extract.

Using the utsrestore i Command

The following procedure demonstrates hosy to use the ufacest ore i command to extract individual files from a backup tape.

Become the rock user, and change to the temporary directory that you want to receive the extracted files.

cd /var/tmp

Perform the ulsrestors i command.

ufsrestore ivf /dev/rmt/0

Verify volume and initialize maps

Media block size is 64

Dump date: Fri Jan 25 4:38:53 2002

Cumped from: the ecoch

Level 0 many of /export/home on sys43:/dev/dsk/c0t0d0s7

Label: TORE

Extract directories from tape

Emitialize symbol table.

3. Display the contents of the directory structure on the backup tape.

ufsrestore > le

2 4./ 13 directoryl 15 directory3 17 file2 2 * . . / 10 fil∈l 14 directory2 12 file3

4. Change to the target directory on the backup tape.

utpressore > cd directoryI ufarestere > le ./directaryl:

3904 ./

3905 file1

3996 file2

3907 file3

5. Add the files you want to restore to the extraction list.

ufsrestore > add file1 file2 Make node ./directoryi

> Files you want to restore are marked with an asterisk (*) for extraction. If you extract a directory, all of the directory contents are: marked for extraction.

In this example, two files are marked for extraction. The 1s command displays an asterisk in front of the selected file names, file1 and file2.

ufsrest, ere > la

./directoryl: 3904 *./

3906 *file2

3907 file3

6. To delete a file from the extraction list, use the delete command.

ulsrestore > delete file1

The 1s command displays the fale! file without an asten'sk.

ufsrestere > 1s

./directoryl:

3904 4./

3905 f 1 3905 *file2 3907 f!le3

To view the files and directories marked for extraction, use the cartes command.

_fsrestore > marked

./directoryl;

3904 +./

3906 *file2

To restore the selected files from the backup tape, perform the command:

ufgrestore > excract

Extract requested files:

You have not read any volumes yet.

Unless you know which volume your file(s) are on you should start with the last wolome and work towards the first.

Specify next volume #: 1



Note — The ufsizestone command has to find the selected files. If you used more than one tape for the backup, first insert the tape with the highest volume number and type the appropriate number at this point. Then repeat, working towards Volume #I until all files have been restored.

extract file ./directoryl/file2

Add Links

Set directory mode, owner, and times.

set www.mer/mede for '.'? lynl n



Note - Answering y sets ownership and permissions of the temporary directory to those of the directory structure on the tape.

 To pair the interactive restore after therities are extracted, perform the command:

utsrestores quit

- Move the restored files to their original or permanent directory location, and delete the files from the temporary directory.
- # my /var/top/directory1/file2 / figert/home
- i m -r /var/tmp/director/1



Note - You can use the help command in an interactive restore to display a list of available commands.

Performing an Incremental Restore

When performing incremental restores, start with the last volume and work towards the first. The system uses information in the mestoresymmable file to restore incremental backups on top of the latest full backup.



Note – If you perform an incremental restore of data from backup tapes that were written from an active file system, the ufsrest.ore command might become disrupted.

Perform; PG File System Acatoms
Coggright 2008 Sun Microsystems, Inc. All Rights Hetained, Sun Services, Revision 7-2

The following protedure demonstrates how to restore the /expent/home file system from incremental tapes.



Note — This procedure makes use of the interactive rectors to assist in showing the concept of incremental restores. You would typically use a command, such as ufsitestone rf, for restoring entire file systems.

 View the contents of the /etc/chowlates file for information about the /epport/home file system.

more /etc/dwmlates grep c0t0d0s7

/dev/rdsk/c0t0d0s7 /dev/xdsk/c0t0d0s7 ● Hen Jan 25 13:10:32 2002

1 Mon Jan 28 13:12:41 2002

 Create the new file system structure for the /export/home file system.

newfs /dev/rdsk/c0t0d0s7

3. Mount the file system and change to that directory.

mount /dev/dsk/c0t0d0s7 /export/home

cd /export/home

- 4. Insert the Level C buckup tape.
- Restore the /export/home file system from the backup tapes.

s ufgrestore rvf /dev/rmt/0

Verify volume and initialize maps

Media block size is 64

Dung date: Wed Apr 03 09:55:34 2002

Dumped from: the 200ch

Level 0 many of /expost pone on sys41:/dev/dak/c0t0d0s7

Label: noneg

Begin level 0 restore

Intialize symbol table.

Extract directories from tape

Calculate extraction list.

Muke noāe ./directoryi

Make node ./directory2

Make node ./directory! Extract new leaves.

Check pointing the restore

extract file ./file1

extract file ./file2

extract file ./file2

Add links

Set directory mode, owner, and times.

Theck the symbol table.

Check pointing the restone

6. Load the next lower-level tape into the tape drive.

ufsrestore rvf /dev/xmt/0

Verify volume and initialize mage

Media block size is 64

Dump date: Wed Apr 03 09:57:30 2002 Dumped from: Wed Apr 03 09:55:34 2002

Level 1 dump of /emort/home on sys41:/dev/dsk/c0t0d0s7

Label: none

Begin incremental restore

Initialize symbol table.

Extract directories from Tabe

Mark entries to be conoved.

Calculate .node updates.

Make mode ./directory4

Make mode ./directory5

Make mode ./directory6

Find unreferences names.

Remove old nodes (directories).

Extract usw leaves.

Check pointing the restore

extract file ./file4

extract file ./file5

extract file ./file6

Add links

Set directory mode, owner, and times.

Check the symbol table.

Check pointing the restore

#

Alternative Steps

The following steps are an alternative to the previous Steps 5 and 6.

Restore the /export/time file system from the backup tapes. (This
exemple uses an interactive, verbose restore to provide more detailed
intermation.)

uferestore iv /dev/smt/0

Verify volume and initialize maps

media block size is 64

Dump date: Mon Jan 28 13:10:12 2002

Damed from: the epoch

Level 0 damp of /export/r.mme on sys41:/dev/dsk/c0t0d0s7

label: none

```
Extract directories from tape
Initialize symbol table.
uferestore > 1s
     2 -./
                          8 dinectory2
                                              5 £5.1e2
     2 4../
                          9 oirectory3
                                               6 file3
     7 directoryl
                          4 file1
                                               3 logi found/
                  The system lists files from the last Level @ backup.
uffrestore > add +
Warning: ./lost+found: File exists
ufarestore > extmact
Extract requested files
You have not mead any volumes yet.
Unless you know which volume your file(s) are on you should
with the last volume and work towards the first.
Specify next volume #: 1
extract file ./file1
extract file ./file?
extract file ./tile3
extract file //directoryl
extract file ./directory2
extract. file ./directoryl
Add links
Set directory mode, ower, and times.
set cwner/mode for '.'? [yn] n
Directories a ready exist, set modes anyway? by
ufsrestore > q
              6. The information in the /etc/duredates file shows an incremental
                  backup that was taken after the Level 0 backup. Load the next tape
                  and perform the incremental restore.
# uferestore 1v
Verify velume and initialize maps
Nedia black saza is 64
Cump date: Mon Jan 28 13:12:41 2002
Dungses from: Mon Jan 28 13:10:12 2002
Level 1 dump of /export/hurmeon sys41:/dev/dak/c0t0d0s7
Label: Hone
Extract directories from take
Initialize symbol table.
uisrestoro > la
     2 = _/
                       13 directory
                                           15 sirectory4
                                                               11 file5
     2 * . . /
                       14 director3-5
                                            1C file4
                                                                12 file6
```

ufsrestore > add * uferestore > extract Extract requested files You have not read any volumes yet. Unless you know which volume your file(s) are on you should start with the last volume and work towards the first. Specify next velume #: 1 extract file ./file4 extract file ./file5 extract file ./file6 extract file ./directory4 extract file ./directery5 extract file ./directofy6 Add 15 tiles Set directory mode, owner, and times. set camer/mode for '.'? [ynl n utsrestere > q

Performing the Exercises

You have the option to complete any one of three versions of a lab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guidance. Each bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab provides more guidance. Although
 each step describes what you should do, you must determine the
 commands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because each step provides exactly what you should input to the system. This level also includes the task solutions for all three levels.



Exercise: Recovering Backup Files and File Systems (Level 1)

In this exercise, you mad the backup tape from the previous exercise. You back up the / (root) file system, restore a single file from tape, and destroy and restore the / (root) file system.

Preparation

This exercise requires a system that is configured with a tape drive and a / (root) file system that is separate from the /use and /var file systems. Identify the slice that holds the / (root) file system. From your instructor, get a tape appropriate for your system.

Tasks

Complete the following:

 Read the contents of both ussues files on the backup tape written in the previous course.

(Steps L-3 in Task 1 of the Level 2 lab)

Reboot the system to run level S. Use the ufsdome command to create a backup tape of the ((root) file system on your system. Verify that the tape combins valid data for this file system. Allow the system to continue to boot to run level 3.

(Sleps 1-5 in Task 2 of the Level 2 lab)

• Use the userestore i command to restore the /etc/inet/nosts file from tape, and place it below the /var/tap directory.

(Steps 1-6 in Task3 of the Level 2 lab)

Remove the /kernel, /platform and /devices directories recursively. About the operating system, and altempt to boot the system from disk. Record what happens. Boot the system from the Solaria 9 Software 1 of 2 CD-ROM to run level. S. Create a new file system on the / (root) slice. Use the ufsrestore command to navad the / (root) file system. Install a new boot block. Reboot the system, and eject the CD-ROM.

(Steps 1-1) in Task 4 of the Level 2 lab)

Exercise: Recovering Backup Files and File Systems (Level 2)

In this exercise, you read the backup tape from the previous exercise. You back up the / (root) file system, restore a single file from tape, and destroy and restore the / (root) file system.

Preparation

This exercise requires a system that is configured with a tape drive and a / (root) file system that is separate from the /use and,/vac file systems. Identify the slice that holds the / (root) file system. From the instructor, set a tape appropriate for your system.

Task Summary

In this exercise, you accomplish the following.

- Read the contents of both afsamp thes on the backup tape written
 in the previous exercise.
- Reboot the system to run level 5. Use the ussue currend to create a backup tape of the f (root) file system on your system. Verify that the tape contains valid data for this file system. Allow the system to continue to boot to run level 3.
- Use the ufsrestore i command to restore the /etc/inet/hosts file from tape, and place it below the /var/tmp directory.
- Remove the Account, Aplatform, and / devices directories recursively. Aborting operating system, and attempt to boot the system from disk. Record what happens. Boot the system from the Solaris 9 OE Software 1 of 2 CD-ROM to run level 5. Create a new file system on the / (root) slice. Use the ufsrestore command to reload the / (root) file system. Install a new boot block. Reboot the system, and eject the CD-ROM.

Tasks

Complete the following tasks.

Task 1 - Read Your Previous Backup Tape

Complete the following steps:

- Locate the backup tape written in the previous emercise, and load it into your tape drive.
- Use the interactive restore command to view the content of he first Level 0 backup tape. Verify that the files are from the /export/home directory that you backed up. Enter q to quit the interactive restore.
- Using a non-rewind device, movethe tape to the next record, and view the contents of the second, incremental backup. Verify that the files you see are from the incremental backup. (The usep directory is the one you added after the Level 0 backup.)

Task 2 - Create a Backup of the / (root) File System

Complete he following steps:

- 1. Log in as the root user, and open a terminal window. Shut down the system to run level 0. Then, boot the system to run level 5. Supply the root password as required to enter run level 5.
- 2. Verify that a tape is in your tape drive.
- 3. Use the utsalum constraind to create a backup tape for the / (root) filesystem.
- 4. Saify that the / (root) file system is on the tape.
- 5. Allow the system to continue to boot to run level 3.

Task3 - Restore the /etc/inet/hests File From a Tape

Com lete the following steps:

- Log in as the root user, and open a terminal window. Change to the /var/tmp directory.
- Enter the ufsrestore in command to retrieve the /etc/inet/hosts file from the tape.
- 3. Change to the /eto/inet directory on the tape, and list the files in the directory.

- 4. Add the Bosts file to the list of files to extract, and display the list.
- 5. Extract the house file from tape. Specify volume number 1. Do not set the owner and mode for ., and then quit the unsrestone command.
- Verify that the etc/inst/closts file exists below the /ver/inst directory.

Task 4 -- Destroy and Restore the / (root) File System

Complete the following steps:

- Change to the / (most) directory, and remove the following critical system directories and their contents: /kernel, platform, and /devices.
- 2. Press the Stop-A key sequence to about the operating system.

 Attempt to boot the system from the boot disk.
 - What happens?
- 3. Invert the Solaria 9 Software 1 of 2 CD-ROM. Boot the system from the CD-ROM to run levels.
- 4. Use the next a command to create a new file system on the / (root) slice. (The slice should match the one you used earlier in the exercise when you created a backup of the / (root) file system.) Run the tack command on the file system that you create.
- 5. Verify that your root backup type is in the tape drive. Mount the new file system as the /a file system. Change to the /a directory.
 - 6. Use the userstore command to load the / (root) data into the new file system.
 - 7. Remove the restoresymtable file.
 - Thistell a new boot block in Sectors 1 through 15 of the / (root) sice, by changing to the directory containing the boot block and entering the install boot command.

od /usr/platform/'uname -m'/lib/fs/ufs

- # installboot bootblk /dev/rdsk/c0t0d0s0
 - 9. Change to the / (root) directory, and unmount the new file system.
 - 10. Reboot the system.
 - Log in as the root user, and open a terminal window. Eject the Solaris 9 Software 1 of 2 CD-ROM.

Exercise: Recovering Backup Files and File Systems (Level 3)

In this exercise, you read the backup tape from the previous exercise. You back up the / (root) file system, restore a single file from tape, and destroy and restore the / (root) file system.

Preparation

This exercise requires a system that is configured with a tape drive and a / (root) file system that is separate from the /usr and /var file systems. Identify the slice that holds the / (root) file system. From the instructor get a tape appropriate for your system.

Task Summary

In this exercise, you accomplish the following:

- Read the contents of both ufsdump files on the backup tape written in the previous exercise.
- Reboot the system to run level S. Use the infadure communic to create a backup tape of the / (root) file system on your system. Verify that the tape contains valid data for this file system. Allow the system to continue to boot to run level 3.
- Use the ufsrestore i command to restore the /etc/inet/hosts file from tape, and place if below the /war/tmp directory.
- Remove the /kennel, /platform, and /devices directories recursively. Abort the operating system, and attempt to boot the system from disk. Record what happens. Boot the system from the Solaris 9 Software 1 of 2 CD-ROM to run level S. Create a new file system on the / (root) slice. Use the ufsrestore command to reload the / (root) file system. Install a new boot block. Reboot the system, and eject the CD-ROM.

Tasks and Solutions

Complete the following tasks.

Task 1 - Read Your Previous Backup Tape

Complete the following steps:

- 1. Locate the backup tape written in the previous exercise, and load it into your ape drive.
- Use the interactive restore command to view the contents of the first Level 0 backup tape. Verify that the files are from the /export/come directory that you backed up. Enter q to quit the interactive restore.

```
# ufsrestore iv
```

```
Verify volume and initialize maps

Media block size is 64

Ourse date: Fri Jan 25 08:38:53 2002

Dumped from: the epoch.
Level 0 clump of /export/home or sys43:/dev/dsk/c0t0d0s7

Labsl: none

Extract directories from tape

Initialize symbol table.

ufsrestore > 1a

...

2 *./

3712 default/ 6 file3

2 *../

4 file1 3 lost+found/
```

file2

You should see the files from your /export/home directory.

ufsrestore > quit

cere

 Using a non-rewind device, move the tape to the next record, and view the contents of the second, incremental backup. Verify that the files you see are from the incremental backup. (The cusp directory is the one you added after the Level 0 backup.) Quit the interactive nestore.

mt _f /@ev/rmt/0n fef 1 # ufsreatore ivf /dev/rmt/0

Verify volume and initialize maps

Media block size is 64

Dump date: Pri Jan 25 08:41:12 2002

Dumped from: Pri Jan 25 08:38:53 2002

Level 1 dump of /export/home on sys43:/dev/dsk/c0t0d0s7

Label: none

Decract directories from tape

Initialize symbol table.

ufsmestore > 1s

2 4.17

7424 uucp/

ulsrestore > q

#

Task 2 - Create a Backup of the / (root) File System

Complete the following steps:

 Log in as the root user, and open a terminal window. Shut down the system to run level 0. Then boot the system to run level 8. Supply the root password as required to enter run level 8.

init 0

(shutdown messages)

ok boot -s

- 2. Verify that a tape is in your tape drive.
- Use the unsalimp command to create a backup tape for the / (most) file system.

wfedump Ouf /dev/rdc/cotodoso

4. Verify that the / (root) file system is on the tape.

uferestore tvf /dev/ret/0

The screen should scroll directory structures under / (reot) first, followed by files.

5. Allow the system to continue to boot to run level 3.

Control-D

Task3 - Restore the /etc/inet/hests File From a Tape

Complete the following steps:

 Log in as the root user, and open a terminal window. Change to the /var/t.up directory.

cd /var/tmp

Enter the affectione i command to retrieve the /=tc/inet/hosts file from the tape.

uferestore if /dev/mut/0

ufstestorie > 16

You should see files and directories for the 1 (root) file system.

 Change to the /etc/inst directory on the tape, and list the files in the directory.

ufarestore > cd /etc/inet

uffreshore > 1s

You should see files and directionies for the /etc/inet file system.

4. Add the hoses file to the list of files **extract, and display the list.

uffrestere > add hosta

You should see the hoses file listed.

5. Extract the hosts file from tope. Specify volume number 1. Do not set the owner and mode for ., and then quit the utsrestore command.

ufsrestore > extract

Extract requested files

You have not read any volumes yet.

Unless you know which volume your file(s) are on you should start with the last volume and work towards the first.

Specify next volume 4: 1

set owner/mode for '.'? [yn] n

uforestore > q

 Verify that the etc/inet/hosts file exists below the /var/tage directors.

ls etc/inet/bosts

etc/inet/hostm

Task 4- Destroy and Restore the / (root) File System

Complete the following steps:

 Change to the / (root) directory, and remove the following critical system directories and their contents: /kern51, /platform and /devices.

cd /

m -r /hamal /platform /devices

Press the Stop-A key sequence to about the operating system. Attempt to boot the system from the boot d'isk.

ok boot

What happens?

The system fails to boot and displays the message.

Boot load fuiled.

The file just leaded does not appear to be executable

 Insert the Solaris 9 Software 1 of 2 CD-ROM. Boot the system from the CD-ROM to run level S.

ck boot edram -B

- 4. Run the nexts command to create a new file system on the / (not) slice. (The slice should match the one you used earlier in the exercise when you created a backup of the / (root) file system.) Enter the issk command on the file system that you create.
- # newfs /dev/rdsk/c0t0d0s0
- # fsck /dev/rdsk/c0t0d0s0
 - Verify that your root backup tape is in the tape drive. Mount the new file system as the /a file system. Change to the /a directory.
- # mount /dev/dsk/c0t0d0s0 /a
- al bo in
- Use the ufsrestore command to load the / (root) data into the new file system.
- t ufsrestore rf /dev/mt/0
 - 7. Remove the rest === yarable tile.
- # zm restoresyntable
 - Install a new boot block in Sectors 1 through 15 of the / (root) slice, by changing to the directory containing the boot block and entering the install boot command.
- i cd /mar/platform/`uname -m`/lib/fs/ufs
- # installbook boothik /dev/rdak/c0t0d0s0

- 9. Change to the / (root) directory, and unmount the new file system.
- i ed /
- # unount /a
- 10. Reboot the system.
- Finit 6
- 11. Log in as the root user, and open a terminal window. Eject the Solaris 9 Software 1 of 2 CD-ROM.
- # eject chron



Exercise Summary



Discussion - Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercises.

- Experiences
- Interpretations
- Conclusions
- Applications



Introducing Disaster Recovery Fundamentals

This section introduces some basic concepts and criteria for the planning and anticipation of a disaster. Understanding what disaster recovery is slowed be the first step you take toward defining and implementing a disaster recovery plan.

Identifying the fundamentals of a disaster recovery plan start with defining what a disaster is. In most cases, it can be defined as follows: any unplanned, extended loss of critical business applications due to a lack of computer processin capabilities. In this definition, extended is defined by the individual business at hand. Some businesses might suffer severe losses in one hour while other businesses might not suffer severe losses.

Disaster Scenarios That Can Result in a Loss of Data

Disasters, both natural aid man-made, happen every day. For example, flooding in Chicago might discrept operations in 400 data centers in Chicago or all over the United States, or a hurdicane could disable the reservation system of a major airline. A major storm could interrupt power to a geographic area for an extended period of time. A fire could destroy business critical infrastructure.

Many Ecnarios could involve the loss of major components of a business-critical system or systems. You have many ressons to consider having a well-thought-out disaster recovery plan in place. The most important reasons might be the ones you cannot think of.

Disaster Recovery Plan

No single document can present a comprehensive analysis of how to prepare a disaster recovery plan. However, this section describes some of the key steps to create a plan.

Solicit D partment Input

Gather input from the departments within your company. Individuals in these departments know the type of data they create and the importance of the data. If you work at a large company, you might organize a planning team so that the telamoan inform management on the status of the disaster recover program. Departments might be tasked to complete periodic tests to verify implementation of the disaster recovery program. The departments can present any findingsof gaps or risks they excounter.

Acquire Management Approval

Involve management early in the decision-making process. This is an important step if you are to obtain the necessary resources and time required from each area of your organization.

You, or your planning team, should complete a study of the disaster recovery plan and include an estimate of the cost of a disaster, as well as an estimate of the possible costs and time to implement a disaster recovery strategy. When management understands the financial, physical, and business costs associated with a disaster, the planning team is able to build a strategy and ensure that the strategy is implemented across the organization.

Develop a Budget

Cost-justifying a diseaster recovery, program is relatively simple. No competitive organization can afford to be without a comprehensive program. In developing a budget for your program, you should consider the following:

· Your current cost of downtime

Look at both the total cost per minute as well as the cost per event, and include the intempible or soft-dollar costs, such as loss of productivity and diminished customer candidarce.

The cost of re-creating data

Consider the time lost re-creating files, the expense of retrieving data from crashed hard disks, the cost of unavailable data when you need it, and the additional costs involved in re-creating lost data when there is no backup copy available.

The cost of expert assistance

Compared to the costs of downtime, the costs of hiring experts to assist with the disaster recovery program are minimal.

Evaluating the Critical Factors for the Plan

Creating the actual disaster recovery plan varies from one company to another. Every company must first evaluate the following critical factors for a disaster recovery plan:

What is the greatest risk?

Is your company most susceptible to natural events, such as corthquales, fires, or floods; mechanical failures, such as hardware and software problems; human error; or intrusions, such as hardware attacks and viruses?

- How are various groups or departments within your cumpany affected by downtime?
 - For each group, how vital is access to data?
 - How long could each group or department function without access to data?
 - Is the hypeware and data all centrally located, or are there alternative sites or departments that can provide the resources lost in the event of a disaster?
- What preventative measures are in place right now?
 - Is there a disaster team?
 - Have you defined a backup strategy?
 - There is the most valuable data stored, and is it adequately protected?
 - Have you documented inventory with schematics, specifications, passwords, menus, utilities, and startup files?
 - Do your facilities have backup data lines and connections?
- How can you recover your data?
 - Who is in change of managing this process?
 - Is there a consmunication procedure?
 - Could you recover your data at a different facility or geographical area or with different personnel?
 - Do you have the need for a hotsite? If so, do you establish the hotsite or use a hotsite vendor?
 - How long would it take to fix your existing facility under various disaster scenarios?

- Should you out-source the data recovery process to a third-party company?
- Do you have emergency contacts with your suppliers?
- What are the approval procedures for emergency planning?
- What happens if you cannot reach key personnel?

Create a Procedure

After you have analyzed the previous choices, you are ready to establis the actual procedures that you must follow in the event of a disaster. The procedures must:

- Define how to andle various aspects of the network, including loss
 of servers, bridges and routers, communications links, and so on
- Specify who arranges for repairs or reconstruction and how the data recovery process occurs
- Include a checklist or test procedure to verify that everything works when the repairs and data recovery have taken place

Test the Procedure

You must test the plan—not just once, but often. You should determine requestly you test the plan, by considering the following factors:

- Personnel changes
- · System changes
- Network changes

You must measure the success of each test. You must define the objective measurements to verify that your plan is effective.

Keep Pace With Changes

Change is the only constant in the corporate world, and it is important that your disaster recovery plan takes into account the impact of change. Consider the following:

- Are there processes in place to include new departments and facilities in the disaster recovery plan?
- Is there a regularly scheduled review of the plan?
- Who maintains the disaster management team roster?
- Could someone new execute the plan?
- How do you conununicate changes or modifications to the plan to people who are affected by the changes?

Importance of Off-Site Backups

Having a comprehensive and quality backup program is vital to a good disaster recovery gian. The value of backed-up data depends on the security and physical protection of that media.

Many scenarios can account for data loss or comption. These scenarios fall short of what is typically considered a disas er. In some instances, you might need to recover data lost due to human error or a minor hardware feiture. To recover from data corruption you need to gain quick access to backup media, such as tape.

Many Information Technology (IT) providers keep a local copy of their backups and send a tested copy of the same backups to an oif-site storage service provider. Off-site storage gives you the opportunity to keep an integrity-tested copy of all your data in a safe locatin laway from the site of business. Off-site providers store your backups in a disaster-ready environment. These sites usually are built to protect your backups from most known disaster scenarios, such as fire, flood, theft and so on. Without an off-site storage solution, you could place even the most comprehensive disaster recovery program at great risk.

Components Required to Operate a Hotsite

You might decide that there is sufficient need and business justification to implement a hotsite as part of your disaster recovery plan. A hotsite is a virtual replication of your critical business computer operations. A hotsite is also known as a disaster recovery site.

If the cost of establishing a hotsite is too high, you can use commercial hotsite vendors. Some disaster recovery vendors offer a variety of options. In a hotsite environment you might get pre-installed computers, networking equipment, telecommunications equipment, raised flooring, air conditioning, technical support, and uninterruptable power supplies.

Importance of Disaster Recovery Drills

As part of a comprehensive disaster recovery plan, testing is one of the most critical steps. After successfully testing your disaster recovery plan, you must continue to test your plan on a regular basis through disaster recovery drills.

Conducting disaster receivery drills allows you the opportunity to adjust and update your disaster seconery plan as needed. You have the opportunity to account for personnel changes, system changes, application changes, and so on.

Conclusting disaster recovery drills on a regular basis also keeps the importance of disaster recovery as a priority in your every day computer operations. The more you practice for disaster recovery scenarios, the quicker you are able to recover, saving more of your customer base and your business earnings.

Backing Up a Mounted File System With a UFS Snapshot

Objectives

Upon completion of this module, you should be able to:

- Create a UFS snapshot
- Back up the snapshot file

The following course map shows how this module fits into the current instructional goal.

Performing System Backups and Restores

Performing File System Backups

Performing File System Restores Eacking Up a Mounted File System With a UFS Snapshot

Figure 17-1 Course Map

Creating a UFS Snapshot

The UFS Copy on Write Snapshots feature provides administrators of non-enterprise-level systems an online backup solution for u.ts file systems. This utility enables you to create a point-in-time copy of a ufa file system, called a snapshot as an online backup. You can create the backup while the file system is mounted and the system is in multiuser mode.



Note — The LEFS snapshots are similar to the Instant Image product.

Instant Image allocates space equal to the size of the entire file system that is being captured. However, the file system data saved by UFS snapshots occupies only as much disk space as needed.

Using the fssnap Command

You use the fissing command to create, query, or delete temporary readonly snapshots of uts file systems.

The kurman for the tesmap command is:

/usr/sbin/fssman -F FSlyre -v -o special option(s) mount-point | special

Table 17-1 shows some of the options for the fasmap command.

Table 17-1 Options for the fasmer Command

Option	Description
-d	Deletes the snapshot associated with the given file system. If the -o unlink option was used when you built the snapshot, the backing-store file is deleted together with the snapshot. Otherwise, the backing-store file (which contains file system data) occupies disk space until you delete it manually.
-F FSType	Specifies the file system type to be used.
-i	Displays the state of an FSType snapshot.
-A	Echoes the complete command line but does not execute the command.
-0	Snables you to use special_options, such as the location and size of the backing-store (bs) file.

To create a UFS snapshot, specify a backing store path and the actual file system to be captured. The following is the currenant format:

feenap -F wfs -o be=backing store path /file-system



Note - The backing store wath can be a raw device, the name of an existing directory, or the name of a file that does not already exist.

The following example uses the fissnapcommand to create a snapshot of the /exports/home file system.

fsamap -F ufs -o bs=/var/tmp /amport/home /dev/fssnap/0

The snapshot subsystem saves file system data in a file called a backing-store file before the data is overwritten. Some important aspects of a backing-store file are:

- A backing-store file is a bit-mapped file that takes up disks pace until
 you delete the UPS snapshot.
- The size of the backing-store tile varies with the amount of activity on the file system being captured.
- The destination path that you specify on the fishing command line must have enough free space to hold the backing-store file.
- The location of the backing-store file must be different from that of the file system you want to capture in a UFS snapshot.
- A backing-store file can reside on different types of file systems, including another use file system or a mounted rise file system.

The feenap command creates the backing-store file and two read-only virtual devices. The block virtual device, /dev/fesnap/0, can be mounted as a read-only file system. The new virtual device, /dev/rfssnap/0, can be used for raw read-only access to a file system.

These virtual devices can be backed up with any of the existing Solaris Oli backup commands. The backup created from a virtual device is a backup of the original file's ystem when the UFS snapshot was taken.



Note – When a UFS snapshot is first created, the file yetem locks temporarily. Users might notice a slight pause when writing to this file system. The length of the pause increases with the size of the file system. There is no performance impact when users are reading from the file system.

Limiting the Size of the Backing-Store File

Before creating a UFS snapshot, use the df. -k command to check that the backing-store file has enough disk space to grow. The size of the backing-store file depends on how much data has changed since the previous snapshot was taken.

You can limit the size of the backing-store file by using the -a maximum option of the fissner command, where a (k, m, or g) is the maximum size of the backing-store file specified in Kbytes, or Gbytes.

Additionally, you can place a minimum size on the backing-store file by using the -o ministre=noption with the fashap command.



Caution — If the backing-store the runs out of disk space, the system automatically deletes the UPS snapshot, which causes the backup to fail. The active uta file system is not affected. Check the /var/asm/messages file for possible UPS snapshot errors.



N te -- You can force an unmount of an active use file system, for which a snapshot exists (for example, with the unount -- f command). This action deletes the appropriate snapshot automatically.

The following example creates a snapshot of the /expert/home file system, and limits the backing-store file to 500 Mbytes.

fssnap -F wfs -o bs=/var/tmp,namsize=500q /amport/home /dev/fssnap/0

Displaying Information for a ufs File System Snapshot

You can use either fastrap command to display UPS snapshot information.

The following example displays a list of all the current UFS snapshots on the system. The list also displays the corresponding virtual device for

famap -1

- n /expcrt/home
- /usr
- 2 /database

You use the -1 option to the /usr/11b/fs/ufs/fssnap command to display detailed information for a specific UFS snapshot that was created by the issue command.

The following example shows the details for the /exact/t-one snapshot.

/uar/lib/fs/ufs/fssnap -i /emport/home

Snapshot number Black Pevice Raw Device Mount point Device state Backing store path

Backing store size Maximum backing store size

Shapehot creace time Copy-en-write granularity

i /der/fssnap/e

: /dev/rfcspap/0 : /export/home

: iele :/var/tmp/snapshot0

; 0 KP : 512000 KB

: Man Per 22 08:58:33 2002

32 HB

Backing Up the UFS Snapshot File

The virtual devices that contain the UFS snapshot act as standard read-only devices, which enable you to back up the virtual device in the same manner as you would back up a file system.

Performing a Backup of a UFS Snapshot

You can use the tar command or the ufsdum conunand to back up a UFS snapshot.

Using the tar Command to Back Up a Snapshot File

If you use the tar command to back up the UPS snipshot, mount the snapshot before backing it up. The following procedure demonstrates how to do this type of mount.

- 1. Create the mount point for the block wirtual device.
- alight -p /backupa/home.bioto
 - 2. Mount the block virtual device to the mount point.
- # sount -F ufs -o ro /dev/fssnap/o /hecomps/home.blom
 - 3. Change directory to the mount point?
- # cd /haclospe/home.bloup
 - 4. Use the tax command to write the data to tape.
- # tar cvf /dev/IMC/G .

Using the ufsdurp Command

If you use the utsaum command to back up a UPS snapshot, you can specify the raw virtual device during the backup.

afodump Out /dev/zmt/0 /dev/zfasmap/0

Verify that the UFS snapshot is backed up.

f ufsrestore tf /dev/rmt/0

Performing an Incremental Backup of a UFS Snapshot

Incremental snapshots contain files that have been modified since the last UFS snapshot. You use the ufsdume command with the N option to create an incremental UFS snapshot, which writes the name of the device being backed up, rather than the name of the snapshot device to the /etc/dumpdates file.

The following example shows how to use the ufectuap currented to create an incremental backup of a file system.

ufsdum lufN /dev/rmt/0 /dev/rdsk/clt0d0s0 /dev/rfssnap/0

Next you would verify that the UFS snapshot is backed up to tape.

uncestare tf /dev/mt/0

To understand incremental backups of snapshots, consider the following demonstration:

 Create a snapshot of the /extra file system that is going to be backed up while the file system is mounted.

fssnap -o be=/ver/tmp /entra

/dev/fss/140/0

 Verify that the sna.pshot was successful, and view detailed information about the snapshol.

fssnap -1

0 /extra:

* /usr/lib/fs/ufs/fssnap -i /extra

Snapshot riudicer

Flock Device : /dev/fssmap/0
Raw Device : /dev/rfssmap/0

Mount point: :/extra

Device state : idle

Packing store patr. : /var/amp/snaretot0

Hamitum backing store size : 0 KB

Snapshot create time : Thu Apr 04 10:34:21 2002

Copy-en-write granularity 1 32 KB

 Make a directory that will be used to mount and view the snapshot data.

midde /extrasnap

Backing Upa Mounted File System With a UFS Snapshot Copylght2003 Sun More proventic, at Highs Reserved, Sun Services, Applicance 4. Mount the snapshot to the new mount point, and compare the size of the file system and the snapshot device.

```
# mount -o ro /dev/fssnap/0 /extraanap
```

df -k | grop extra

/dev/dsk/cltCdCs0 1294023 9 1242254 1.9 /extra 9 1242254 /dev/tssnap/0 1234023 13 /EXTrasnap

> 5. Edit a file under the /extra directory and make it larger, and then compare the Size of the file system and the snapshot device.

evi filel

(yank and put text, or read text in from another file)

df -k |grop extra

20 1242243 18 /dev/dslc/clt0d0s0 1294023 Extra 1294023 18 9 1242254 /extrasnap /dev/fssnap/0

Observe that the file system grow in size while the snapshot file did

6. Perform a full backup with the Northern of the ufsaump command.

ufsdwmp OufN /dev/rmt/0 /dev/rdsk/clt0d0s0 /dev/rfssmap/0

DAMP: Writing 12 Milabyte records

DOFF: Date of this level 3 dump: Thu 04 Apr 2002 10:49:38 AM MST

DUMP: Date of last level 0 dump; the epoch

muno: Dumping /dev/rissnap/0 (sys41:/extrasnap) to /dev/mnt/0.

DUME: Mapping (Page I) [regular files]

CURP: Happing (Pass II) [directories]

DUMP: Estimated 262 blocks (131KB).

DUMP: Dumping (Pass III) [directorles]

DUMP: Dumping (Pass IV) [regular files]

DUMP: Tape rewinding

DUMP: 254 blocks (1273) on 1 volume at 1814 KB/sec

DUMP: DUMP IS DONE

DUMP: Level 0 dump on Thm, 04 Age 2002 16:49:35 AM MET

7. Veriff the backup.

uffrestore tf /dev/rmt/0

2

3

./filel ./file2 2

5 ./file3

./file4

#

8. Unmount the back up device and remove the snopshot.

www.t /extrasnap

fammp -d /extra

rm /var/top/snapshot0

#

Make some changes to the /extra file system, such as copying some files, and then re-create the snapshot.

```
# cp filel file5

# cp filel file6

# fganap -o be=/var/tmp /extra
/dev/fssnap/0
```

 Re-mount the snapshot device, and compare the size of the file system and the snapshot device.

```
# mount -o ro /dev/fsenap/0 /extrasnap
# df -k |grep estra
/dev/dsk/clt2d0s0 1294023 45 1242217 18 /extrasnap
/dev/fssnap/0 1294023 46 1242217 18 /extrasnap
```

 Perform an incremental backup with the N option of the ufsaump command.

```
ufschmp luft /dev/rot/0 /dev/rdat/clt0d0s0 /dev/rismap/0

DUMP: Writing 32 Kilebyte records

DUMP: Date of this level 1 dump: Thu 04 Apr 2002 10:59:11 AM MST

DUMP: Date of last level 0 dump: Thu 04 Apr 2002 10:49:38 AM MST

DUMP: Dumping /dev/rfssnap/0 (sys41:/extrasnap) to /dev/rmt/C.

DUMP: Mapping (Pass I) [regular files]

DUMP: Dumping (Pass II) (directories)

DUMP: Dumping (Pass III) [directories]

DUMP: Dumping (Pass III) [directories]

DUMP: Tape rewinding

DUMP: 254 blocks (12783) on 1 volume at 1693 KB/sec

DUMP: App IS DONE

DUMP: Wevel 1 dump on Thu 04 Apr 2002 10:59:11 AM MST
```

12. Verify the backup.

```
4 ufarestore tf /dev/mmt/0
```

7 ./file5 8 ./file6

Notice that the backup of the snapshot contains only the files that were added since the previous Level 0 backup.

Restoring Data From a UFS Snapshot Backup

The backup created from a virtual device is a backup of the original file system when the UFS snapshot was taken.

You restore a UPS snapshot from a backup tape in the same manner as you would the backup of an original file system.

To restore the demo directory from the snapshot backup of the /usz file system, complete the following steps:

- Load the tape that contains the snapshot backup of the /usr file system into the tape drive.
- 2. Change to the /usr file system.

cd /usr

3. Perform the a utsrestore command.

```
# ufsrestore if /dev/rmt/0
ufsrestore > add devo
ufsrestore > extract
Specify next volume #: 1
set **emer/mode for '.'? (yn) n
uisrestore > quit
```

4. Verify that the deno directory exists, and eject the tape.

Deleting a UFS Snapshot

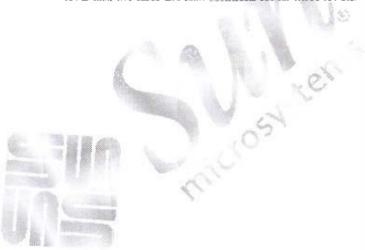
Deleting a LFS snapshot from the system is a multistep process and order-dependant. First, unmount the snapshot device, and then delete the snapshot. Finally, remove the backing-store file.

```
# unount /dev/fssnap/0
# fssnap -d /expert/home
# rm /backing_store_file
```

Performing the Exercises

You have the option to complete any one of three versions of a fab. To decide which to choose, consult the following descriptions of the levels:

- Level 1 This version of the lab provides the least amount of guidance. Each bulleted paragraph provides a task description, but you must determine your own way of accomplishing each task.
- Level 2 This version of the lab provides more guidance. Although
 each step describes what you should do, you must determine the
 cummands (and options) to input.
- Level 3 This version of the lab is the easiest to accomplish because each step provides exactly what you should input to the system. This level also includes the task solutions for all three levels.



Exercise: Working With UFS Snapshots (Level 1)

In this exercise, you create a UFS snapshot of the /out file system, display detailed information for the UFS snapshot, and then remove the snapshot and backing-store file.

Tasks

Complete the following tasks:

- Create a snapshot of the /opt file system.
- Fiew the contents of the backing-store directory
- Display detailed information about the snapshot
- Remove the snapshot from the system



Exercise: Working With UFS Snapshots (Level 2)

In this exercise, you create a UFS snapshot of the /opt file system, display detailed information for the UFS snapshot, and then remove the snapshot and backing-store file.

Task Summary

In this exercise, you accomplish the following:

- Create a snapshot of the /opt file system.
- View the contents of the bac ing-store directory
- Display detailed information about the snapshot
- Remove the snapshot from the system.

Tasks

Complete the following steps:

- 1. Create a snapshot of the /opt file system without specifying afile name for the backing-store file.
- View the contents of the /vac/top file system.
 What is the default name assigned to a backing-store file?
- 3. Display the detailed information about the snapshot.
 What is the maximum backing-store file size for the snapshot?
- 4. Delete the snapshot from the system.
- 5. New the contents of the /vax/top file system.
 Has the backing-store file been removed?
- 6. Remove the backing-store file that you created in Step 1.

Exercise: Working With UFS Snapshots (Level 3)

In this exercise, you create a UFS snapshot of the /opt file system, display detailed information for the UFS snapshot, and then remove the snapshot and backing-store file.

Task Summary

In this exercise, you accomplish the following:

- Create a snapshot of the /opt. file system.
- · View the contents of the backing-store directory
- Display detailed information about the snapshot
- Remove the snapshot from the system#

Tasks and Solutions

Complete the following steps

 Create a snapshot of the /opt file system without specifying a file name for the backing-store file.

fssnap -F wfs -o bs=/var/tmp /opt

- 2. View the consents of the /var/top file system.
 What is the default name assigned to a backing-store file?
 snapshot0
- 3. Display the detailed information about the snapshot.

/usr/lib/fs/ufs/fsamp -i /opt

What is the maximum backing-store file size for the snapshot? Unlimited

4. Delete the snapshot from the system.

fearap -d /opt

Where the contents of the /var /tmp file system. Has the backing-store file been removed?

No

6. Remove the backing store file you created in Step 1.

Im /var/tmp/enapehot0

Exercise Summary



Discussion — Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercises.

- Experiences
- Interpretations
- Conclusions
- Applications



Index

B

level definitions 15-8 numberollapes 15-6 abort key sequence 6-8 remote 15-13 accept command 13-3 restore file system 16-3 accessing removable media 4-25 restoresymtable 16-2 adding software packages restoring snapshot 17-10 communal 6.7 scheduling 15.7 adjusting a link counter 3-20 strategies 15-6 ละเกิดเอเทา 10-5 backup superblock 3-7 administering Volume. banner command 8-12 Management 4-24 bin account 10-5 at command blacks, cylinder group 3-8 allowing access 14-15 tood controlling access 14-14 block 3-7 denying access 14-14 device 9-5 executing 14-13 overview 14-12 disk device path name 8-29 process 9-1, 9-11 autoconfiguration 9-7 secondary program 9-5 automatic execution of boot -a command 9-10 commands 14-15 boot command 2-19, 8-12 boot PROM boot sequence 9-5 commands 8-11 delinition of 8-3 backing-store file overview 8-2 definition 17-3 Sootblk cummand 3-7 limiting size 17-4 bootblk program 9-5 boot d∉vice parameter 8-26 before installation 5-11 budgets, disastor tecovery 16-27 definition of 15-2

bus configuration 2-16

busy file system 4-17

frequency and levels 15-7

full 15-7 incremental 15-7 information 15-9

C	Cinger 11-4
	fmthard 2-50
CDE process manager 14-2	format 2-18, 2-32
CD-ROM	Isck 3-16, 3-17, 3-18, 4-11
drive 4-22	fsenzp 17-2
CD-ROM drive	fssnap -i 17-5
location 4-22	Istyp 4-14
change group command 11-38	fuser 4-17
change owner command 11-36	grey 6-3
Changes 4-10	gre-upadd 10-19
changes in recovery plan 16:30	groupael 10-21
changing default printer 12-,15	groups 11-34
changing NVRAM parameters & 16, 8-27	halt 9-28
thecking	help 8-14
file systems 4-11	14 11-35
software packages cummand 6-8	init 9-26
chgrp command 11-38	kill 145
chown command 11-36	last 11-5
class name 12-31	ln 1-12
cluster configuration 5-5	1p 12-12
command-line tools 10-11	1Bacain 12-34
	I pigove 13-3
.project 11-4	_pr 12-12
/etc/dumpostes 15.9	15.1-8
/eEd/init.d/lp start 12-37	mkdir I-II
/etc/init.d/lp stop 12-37	merint 4-4,4-8, 4-13, 4-25
/usr/dt/bin/ sduprocess 14-2	mt 15-5
/usr/sadmin/cin-	nex1s 3-14, 4-12
printmgr 12-20	severe 10-9
accept. 13-3	nvalias 8-25
at 14-12	nomalias 8-26
barner 8-12	patchadd 7-4, 7-9
boot 2-19, 8-12	eatchen 7-12
200t -a 9-10	pkgadá 6-7
bootPROM 8-11	pkgchk 6-8
bectblk 3-7	pleginto 6-1
cherp 11-38	pkgrm 6-10
chioner 11-36	pezecciá 9-28
compress 15.4	princenv 8-15
devalias 8-24	prebe 8-17
devisadu 2-20	probe toal 8-20
c:f 3-2.3	probe-ide 8-20
disable 13-3	probe acsi 8-19
du 3-25	probe-scsi ali 8-19
eapron 8-27	prstat 14-4
erable 13-3	precent 2-17

	provinc 249	configuration files 4-23
	guet 3-26	consistency
	reboot 9-28	cylinder group black 3-17
	reject 13-3	datableck 3-17
	runount 4-23	inode 3-17
	rusers 11-3	CONSILE variable 11-12, 11-14
	set-dežaults 8-17	controller number 2-8
	setem 8-16	corrupted file sys tem 3-16
	show-devs 8-23	course goals Proface-xix
	show-disks 8-25	creating
	showev 7-4	custom device aliases 8-27
	shutdown 9-26	new run control scripts 9-23
	smgroup add 10-19	printer classes 12-32
	emgreup delete 10-22	procedures for recovery plan 16-29
	sagroup modify IO-21	ufs file systems 3-14
	smuser 10-11	creating mount points 4-12
	amuser add 10-14	creating new file systems 4-12
	smoer delete 10-18	crondaemon 14-15
	squiser modify 10-17	croning file
	su 11-7, 11-10	accessing 14-19
	tar 7-8, 17-6	definition of 14-15
	touch 1-9	
	tunefs 3-15	editing 14-18 format 14-15
	ufologo 15-10, 15-13, 17-6	
		removing 14-18
	uferestore i 16-7	riewing contents 14-17 custonize disk window 5-37
	CMOUNT 4216	
	urumont -f 4-18	cylinder 2-4
	unnountall 4-17	eylinder group block consistency 3-17
	wnzip 7-7	cylinder group blocks 3-8
	useradi 10-13	cylinder groups 3-8
	usermod 10-16	
	usfrestore 16-3	D
	verify 2-48	U
	vcloheck 4-21	dad(direct accessdevice) 2-14
	who 1J-2	dagron account 10-5
	shoani 11-8	daemon, network listening service 12-11
	zcat 7-8	daemons
	mpress command 15-4	/usr/sbin/vold 4-21
30	nfiguration	cren 14-15
	/ecc/systemfile 9-6	in.1pā 12-11
	kernel 9-8	ineto 12-10
	new network printer 12-23 to 12-30	Internet services 12-10
	printer 12-31	ipsched 12-15
	printer services 12-19	network server 11-3
	removing printer 12-35	The misers 11-3
	Volume Management files 4-23	scheduler 12-11

Index-3

data block	/kernel 1-3, 9-6
definition of 3-11	/kernel/dry 9-7
fragmentation 3-12	/rmt 1-3
data block consistency 3-17	/opt 1-3
data blocks 1-7	/platform 1-3
data compression 15-4	/platform/'uname -i'/kernel 9-6
data organization on disk platters 2-3	/platform/'whame -m'/kernel 9-6
date mounted 4-6	/sbin 1-3, 4-4, 9-17
dest'unation printer default 12-34	/aux/share/lib/terminto 12-7
destination printer, locating 12-12	/ETTP 1-3, 1-4, 4-7
devalias command 8-24	/usr 1-3
devisacincommand 2-20	/usr/bin 12-7
device	/usr/kem=1 9-6
dnss 2-20	/usr/kemel/dry 9-7
loading drivers 2-20	/uar/lib@p 12-7
name 4-6	/msr/lib/leg postscript 12-8
naming conventions 2-11	/usr/lib/lg/miel 12-7
path names 8-23	/usr/gbin 12-7
device aliases	/usr/mare/ libterminfo 12-26
creating 8-27	/usr/share/lib/terminfo 12-7
removing 8-26	/var 1-3, 1-4
device configuration tree 2-13	/var/lp/logs 12-10
device dr.ver 2-13	/var/sacm 7-4
device drivers directory 9-7	/var/sadmo/gatch 7-3
device tree 8-21	var/spco1/1p 12-9
df command 3-23	/var/speol/pkg 6-11
DHCT 5-16 ₹	description 1-10
different types of file system 4-13	home 10-2
direct access device (dad) 2-14	lost + forma directory 3-17
directories	make command 1-11
/ 1-3	structure 1-2
/ (roet) 1-2	symbolic l'ules 1-11
/bin 1.4	directory hierarchy 1-2
/dev 1-3, 2-11	directory location, removable media 4-22
/dev/dsk 2-11	disablecommand 13-3
/dev/rdsk 2-11	disaster recovery
/dcvices l-4	changes 16-30
/er:t/1p/fd 12-8	creating procedures 16-29
/etc/init.d 9-22	department input 16-26
/ecc/lp 12-8	develop budget 16-27
/etc/1p/fd 12-9	issues to consider 16-28
/etc/lp/interfaces 12-9	management approval 16-27
/sto/lp/printers 12-9	procedure testing 16-29
/etc/md#.d 9-20	
/exert 1-3	
/name 1-3	

disk backup 2-36 formatting with Solaris Management Console Storage Manager 2-73 label 3-6 labels 2-36 number 2-8 overlapping slices 2-35 partition 2-36 repartitioning 2-36 slide 2-36 undesirable conditions 2-33 wasted space 2-34	diskette drive 4-22 diskette drive, location 4-22 displaying details on all packages 6-5 software package information 6-4 distributed file system 3-2 downloading patches 7-7 dri command 3-25 Dynamic Host Configuration Protoc (DHCP) 5-16 dynamic kentral 9-8
disk blocks 2-4	E
disk label fields 2-49	- / T
disknames	editing /etc/system 9-10
legical 2-11	EDITOR variable M-18
physical 2-12	EEPROM 8-5
disk number	espera command 8-27
IDE 2-8	enable currend 13-3
SC51 2-8	enabling login checking 11-6
disk partitioning	end user system support software
s value 2-44	group 5-7 esszironment variables
blocks 2-12	LPDEST 12-14
cylinders 2-42	PRINTER ,12-14
ilag 2-42	
part 2-42	
procedure 2-39	F
size 2-42	611-41a-4-51-11-2
SMC 2-73	failed login file 11-6
tag 2-42	file system /var/run 4-7
disk platter 2-4 disk slice	backup 15-2
controller number 2-8	
defining 2-33	backup information 15-9 busy 4-17
disk number 2-8	checking 4-II
file system 1-2	corruption 3-16
naming convention 2-8	create new 4-12
offset 2-33	creating a cife 3-14
slice number 2-8	determining the type of 4-13
target number 2-8	disk-based 3-2
disk sp.we	display capacity 3-24
by user command 3-26	distributed 3-2
usage command 3-23	forced warmeum 4-17
disk structure 2-2	HSPS 4-14
disk-based file systems 3-2	manually unmounting 4-16

minfree 3-15	/etc/systemormfiguration 9-6
monitoring 3-23	/etc/vfstab 4-4, 4-13
mount point 4-2	/elc/weld.conficonfiguration 4-23
mounting different types 4-13	/recenfigure 2-19
mounting manually 4-8	/var/admileginlog 11-6
mounting new 4-12	/var/adm/utmpx 11-2
name 15.6	/var/adm/winex 11-5
PCFS 4-15	/var/10/100s/requests 12-10
pseudo 3-3, 4-7	/var/sadm/instail/contents 6-2
restoring 16-3	backing-store 17-3
rest type 9-10	configuration 4-23
state flag 3-16	creating regular files 1-9
structure 1-2	crontab 14-15
UFS 3-2, 3-4	datablocks 1-6
ununount all 4-17	description of 1-8
unnounting 4-16	l'ailed login 11-6
numounting busy 4-17	file names 1-6
virtual 4-4	inodes 1-6
file system inconsistencies	list command 1-8
resolving 3-19	ന്ദ്രേവക് 🛂
files	pepairing 4:19
SECRE/ printers 12-14	Switch user Fig. 11-12
570M8/ .rhosts 11-16	types 1-8
.plar. 11-4	unreferenced 3-19
/ect/vistab 48	finger command 11-4
/etc/cron.d/ab.##Dow 14-14	firshware 8-2
/etc/cron.d/at.deny 14-14	Enthar command 2-50
/etc/default/fa 4-13	Torced unmount 4-17
/etc/default/login 11-13, 11-14	forceload parameter 9-10
/etc/default/p sswd 10-10	format command 2-18, 2-32
/etc/default/su 11-11, 11-12	format hard disk 2-50
/etc/dfs/fscapes 4-13	FFROM 8-3
/etc/format.dat 2-36, 2-45	fragmentation 3-12
/etc/ftmd/ftpusers 11-15	free list 3-20
/etc/group 10-2, 10-3, 10-8	fsck conumand
/etc/hosts.equiv 11-16	definition of 4-11
/etc/inetd.conf 12-10	interactive mode, 3-18
/etc/initkub 9-11,9-15	non-interactive mode 3-17
/eto/mottab 4-6	fack program
/etc/pa ss will)~3	at bootup 3-16
/etc/path_to_inst 2-15	definition of 3-16
/etc/printers.comf 12-14	Iosi+found directory 3-17
/etc/ameun.conf	tssnap command 17-2
configuration +23	Issrap -: command 17-5
/etc/sbadow 10-3, 10-6	fstyp command 4-14
/etc/system 9-8, 9-10	FTP, restricting access 11-15

full backup 15.7 Fuser command 4-17	ineta daeman 12-10 information pane 2-71
genunix static core 9.6 geographic location 5-10 GID 10-2, 10-5 grep command 6-3 group file syntax 10-8 group addcommand 10-19 group del command 10-21 groups command 11-34	init command 9-26 init phase 9-11 init process 9-15 init state 9-3 init states 9-3 init default 9-12 inode allocated and unreferenced 3-19 definition of 1-6, 3-9 direct pointers 3-11 indirect pointers 3-11 inode consistency 3-17 install_pluster 7-14
Н	installation
halt command 9-28 hard disk cylinder 2-4 format 2-50 head actuator arm 2-3 read/write heads 2-3 Slice 2 2-4 structure 2-2 track 2-4 hard sector 2-4 hardware requirements 5-4 head actuator arm 2-3 help command 8-14 help screen 2-67 host IP address 5-10 host name 5-10 HSFS file system 4-14	backup 5-11 custom JumpStart 5-3 hardware requirements 5-4 interactive 5-11 pre-installation 5-10 pre-installation information 5-9 software arrangement 5-5 upgrade 5-27 web version 5-2 WebStart flash 5-3 installation options 5-2 installing patches 7-9 instance names 2-14 integrated device electronics (IDE) 1-15 interactive mode 8-13 Interactive mode 8-13 Internet services daemon 12-10
I	J
i & command 11-35 IDE configuration J-15, 2-9 IDE controller devices 8-20 identifying devices 8-17	Jaz drive 4-22
in, Incidaemon 12-11 incremental backup 15-7 snapshot 17-7 incremental restore 16-9 indirect pointers 3-11	kernel configuring 9-8 genumix 9-6 initialization phase 9-6

indirect pointers 3-11

modules 9-6	M
search path 9.9 kill command 14-9	magnetic tape control command 15-5 make directory command 1-11 management
L	approval for recovery plan 16-27
language 5-10, 5-12	issues to consider 16-28
last command 11-5	preparing for disasters 16-26
line printer command 12-12	minfree space 3-15 mkdirconunand 1-11
link command 1-12	media 9-9
link counter 3-20	modes
list command 1-8	interactive 8-13
listen account 10-5	reconfiguration 8-13
isting	single-user &-13
device path names 8-23	verbose 8-13
NV:RAM parameters 8-15	menitoring
system configuration 2-17	switchuserattempts 11-11
Lacommand 1-12	system access 1122
load device drivers 2-20	Rount
local print process 12-15	checking file system 4-11
location bar 2-71	manually 4-11
logical device names 2-11	options 4-6, 4-9
login device types 11-2	procedure 4-12
displaying activity 11-5.	removable media 4-23
enabiling checking 11-6	mount 4-8,4-25
Tailed 11-6	mount command 4-4, 4-13
problems in CDE 10-33	mountpoint
shell 10-2	/etc/mnttab file 4-6 column 15-6
troubleshooting 10-32	creating 4-12
login device types	definition of 4-2
pts 11-2	mounting process 4-2
term 11-2	nt command 15-5
login ID 10-4	
legin commed 10-32	
logs, printer requests 12-10	N
losses, disasters 16-26	name and in the trans. E 10
Грассочий 10-5	name service type 5-10 navigation pane 2-70
12-command 12-12	netmask 5-19
LP Print Service 13-3	netstandardscript 12-8
1paccin command 12-34 LPDESTenvironment variable 12-44	network listening service daemon 12-11
10 nove command 13-3	network screer daemon 11-3
lin command 12-12	newfs command 3-14, 4-12
Ipsched daemon 12-15	newgrp.command 10-9
Is command 1-8	peaccess account 10-5

nobody account 10-6 nobody4 account 10-6 number account 10-5 nvalias command 8-25 NVRAM changing parameters 8-16, 8-27 chip 8-5 definition 8-5 NVRAM listing parameters 8-15 nvarsalias command 8-26	permissions setgid 11-40 setuid 11-39 Sticky Bit 11-41 physical device names 2-12 physical disk structure 2-2 pkgschd command 6-4, 6-7 pkgschd command 6-4, 6-8 pkgir for command 6-4 pkgracommand 6-4, 6-10 pointers
OpenBuot architecture 6-2 overlapping disk slices 2-35	direct 3-11 incirect 3-11 Portable Open Systems Interface (POSIX) 13-2 PostScript filter programs 12-8 power onself that (POSIT) \$35, 8-6, 8-7, 8-9,
P	9-5
partition table customized 2-46 saving 2-45 PASSED2 variable 11-14 password aging 10-2 10-3 file syntax 10-4 user account 10-2 patch checking current, 7-4 downloading 7-7 formats 7-2 ftp utility 7-5 installing 7-9 removing 7-12 patch ctusters, installing 7-13 patchadd 7-4 patchadd command 7-9 patchracommand 7-12 path names, boot disk 8-29 PCFS file system 4-15 PCMCIA card 4-22 permission denied 10-32	print client 12-2 print client 12-2 print management tools 12-2 Print Manager 12-2, 12-20 print server configuration hierarchy 12-8 definition of 12-2 foult notification 12-5 initialization 12-5 memory 12-20 quening 12-5 spooling space 12-19 tracking 12-5 printserver requirements 12-19 print services, configuring 12-19 printery command 8-15 printer add access 12-22 attached 12-22 changing default 12-35 class 12-31 configuration 12-3 configuring 12-31 configuring network 12-23 to 12-30

load balancing 12-31	/sbin/rc3 9-15
local 12-3	/usr/lib/saf/sac 9-16
locating destination 12-12	/usr/lib/saf/toyman 9-16
network 12-3, 12-22	/usr/spin/shutdown 9-15
print filter descriptor files 12-9	pretat comnaud 14-4
priority 12-32	prtcenf command 2-17
process 12-15	prity too command 2-49
remote 12-3	pseudo file system 3-3, 4-7
remote process 12-17	potation in the property of the
removing a configuration 12-35	
requestlog 12-10	Q
restart command 12-37	, , , , , , , , , , , , , , , , , , , ,
specifying destination 13-2	quot convmand 3-26
subdirectory of local printers 12-9	
system default 12-34	R
temporary shutdown command 12-37	
PRINTER environment variable 12-14	re scripts. See nin control (re) scripts
printers	read/write heads 2-3
netsLandard script 12-8	mebeet: command 9-26, 9-28
PostScript filter programs 12-8	reconfiguration boot 2-19
standard script 12-7	reconfiguration mode 8-13
printers.conf.leyname file 12-14	reconnecting allocated unreferenced
printing	files 3-19
accepting jobs 13-3	recovery plan
clearing hung processes 14-9	approval 16 27
disabling queuing 13-5	budget 16-27
enabling queuing 13-4	changes 16-30
nieving jobs 13-6	cronting procedures 16-29
overview 12-2	input 16-26
rejecth gjobs 13-4	issues 16-28
terminatinga hung login 14-11	testing 16-29
priority of printers 12-32	recovery, special case 16.6
orobe- commands 8-17	regular files 1-9
probe-feal command 8-20	reject command R-3
probe-ide command 8-20	remote
probe-scsi comunand 8-19	backup 15-13
prone-sqsi-allcommand 8-19	displaying users 11-3
precess	print process 12-17
stopping 4-18	remote system users 11-3
testing recovery: 16-29	removable media de vice 4-21
process manager 14-2	removable media, accessing 4-25
process manager window: 14-3	remove software package command 6-10
PROCESS/NEWP 14-5	removing
proceses	custom device aliases 8-26
/sbin/init 9-6	removing a patch 7-12
/sbin/rc2 9-15	repartitioning a disk 2-36

requirements, print server 12-19	scripts scripts
respawn 9-12	netstandard 12-8
restore	n on control (rc) 9-11
/opt file system 16-3	standard 12-7
/uer 16-5	SCSI configuration 2-9
/ugr file system 16-4	SCSI controller devices 8-19
/var 16-5	search path for kernel modules 9-
incremental 16-9	secondary boot program 9-5
interactive 16-7	sector 2-4
regular file system 16-2	set defaults command 8-17
root lile system 16-6	seteny command 8-16
resteresymtabl# file 16-2	setgid permission 11-40
restoring UFS file system 16-2	setuid permission 11-39
restricting #tp access 11-15	shactow file syntax 10-7
pestricting root access 11-13	show-devs command 8-23
ranount command 4-23	show-disks command \$-25
rcot	showrev 7-4
access 11-7	shuzdown command 9-26
account 10-5	shutdown procedures 9-25
file system type 9-10	SIGHUP signal 14-10
password 5-10	SIGINT signal 14-10
restricting access 11-13	SIGKILL signal 14-10
rpc.ruse_rsdlammon 11-3	SIGTERM signal 14-10
RSS 14-4	single-user mode 8-13
run control (rd) scripts	SIZE 14-4
creating 9-23	Slice 2 2-4
definition of 9-17	slice number 2-8
director# 9-22	smgroup add command 10-19
executing 9-11	sogroup delete command 10-22
run control scripts	smgroup modify command 10-21
starting 9-21	sumspaccount 10-6
stopping 🤊 1	swiser add cominand 10-14
rım levels	smiser command 10-11
/etc/inittabfile 9-11	smuser delete command 10-18
changing 9-3	smuser modify conunand 10-17
definition of 9-2	snapsluet
determining current 9-3	backing up 17-6
scripts 9-20	displaying 17-5
rusers command 11-3	incremental backup 17-7
	restoring backup 17-10
•	software
S	adding packages 6-7
galaraging the free list 2.24	administration 6-2
salvaging the free list 3-20	arrangement 5-5
scheduler daemon 12-11	checking packages 6-\$
scheduling backups 15-7	clusters 5-5, 5-6

packages 5-5, 5-6 packages installed 6-2 remove packages 6-10 software groups End User System Support 5-7 software packages 6-2 Solaris Unstall Console 5-13 Solaris Management Co-sole	superblock backup 3-7.3-21 consistency 3-16 corrupted 3-21 definition of 3-7 list alternates 3-21 switch user complete logan 11-7
definition 2-46	log file 11-12
disk tools 2-73	overview 11-7
information pane 2-71	symbolic link
location bar 2-71	creating 1-12
navigation pane 2-70	definition of 1-11
restarting 2-68	ays account 10-5
scheduler tool 14-20	aysinit 9-12
starting 2-66	system access
status bar 2-72 toolbox editor 2-69	munitiving 11-2
	user information 11-4
tools 2-67 usage 3-27	system configuration listing 2-17
view pane 2-7)	System default printer 12-34
Solaris Mariagement Console Users Tool	system shotdown 9-25
addi gauser 10-23	
definition 10-22	T. 150
deleting a user 10-31	
Solaris OE run levels 9-2	tape device 15-3
Solaris OE upgrade 5-4	tape drive control 15-5
special case recovery 16-6	car command 7-3, 17-6
spool directory 6-11	target number 2-8
etandard script 12-7	time mounted 4-6
STATE 145	time zone 5-10
state flag 3-16	touch ammand 1-9
static core 4-6	track 2-4
status bar 2-72	Iroubleshooting, login 10-32
Sticky Bit permission 11-41	tunets command 3-15
stopal) processes 4-18	
Stop key 8-7	U
STREAMS modules 9-14	•
ສນ command 11-7, 11-10	UFS file system 3-2, 3-4, 16-2
subnet mask 5-10	UISbeet program 9-5
SUECGVariable 11-12	ufsdumpcommand 15-10, 15-13, 17-6
suninstall 5-13	ufsreetore command 16-3
SunService program 7-5	uforestere i command 16-7
SurSolve database 7-5	UID 10-2, 10-3
sunurinstall 5-33	Ultra workshitions 8-3
SUNW 6-5	unount command 4-16

unallocated block count 3-20 unix static core 9-6	V
unrount -f command 4-18 unrountall, command 4-17 unmounting file systems 4-16 unmounting process 4-2 unreferenced files 3-19 unz=pcommand 7-7 upgrade live 5-4 standard 5-4 user becoming root 11-10 displaying effective 11-7 displaying information 11-4 displaying real 11-8 home directory 10-2 switching 11-7 switching log 11-12 switching monitoring 11-11	variables CCNSOLE 11-12, 11-14 EDITOR 14-18 PASREQ 11-14 FJUGG 11-12 verbase mode 8-15 verify command 2-46 view paine 2-71 virtual device 17-3 virtual file system table 4-4 volcheck command 4-21 Volume Mana gement administering 4-24 configuration files 4-23 daemon 4-21 definition of 4-21 starting 4-24 stopping 4-24 volume table of contents (VTCC) 2-36, 3-6
switching regular 13-9 user account	volume more obtained (* 100) 2-00/20
command-line tools 10-11 home directory 10-2 login shell 10-2 password 10-2 password aging 10-2	WebStart 3.0 5-2 WebStart Flash in stallation 5-3 who command 11-2
user accounts	wincemi command 11-8
adding a two with Solaris Management Console 10-23	workstations 8-3
creating 10-13 creating a group 10-19	Z
deleting a group 10-21	-
deleting a user with Solaris	zgat command 7-8
Management Console 10-31 managing 10-11 modifying 10-16 user name 10-2	Zip drive 4-22
useraidcommand 10-13	
usexnodcommand 10-16	
uucpaccount 10-5	